初等整数论

CHUDENGZHENGSHULUN

熊全淹

湖北人民出版社

封面设计：蓉乃志



统一书号：[illegible]

定　价：[illegible]

初等整数论

熊全淹

湖北人民出版社

初等整数论

熊全淹

湖北人民出版社出版　湖北省新华书店发行

沔阳县印刷厂印刷

787×1092毫米32开本 5,875印张 124,000字

1982年6月第1版　1982年6月第1次印刷

印数：1—8,200

统一书号：7100·1633　定价：0.63元

序　言

本书是根据武汉大学的初等数论讲义经过修改补充而成. 内容是介绍初等数论的最基本理论和计算方法. 目的在求作高等院校数学专业的基础读本.

在编写时力求叙述简明,说理详尽,多给例题以利自学. 每节附有习题供读者巩固理论, 熟练计算之用, 大都不甚困难. 书末附有解答, 以备读者校核.

初稿承洪伯阳、谭季伟同志提出了很多宝贵意见, 使本书生色不少, 谨在此表示谢忱.

由于水平所限, 书中不论在内容的选择上或次序的安排上, 都存在不少缺点和错误, 希望读者不吝指正.

编　者

1982 年 1 月

目　　录

序　　言
第一章　整除性理论……（1）
§ 1.1　整除性……（1）
§ 1.2　最大公约数、最小公倍数……（6）
§ 1.3　质数、整数的质因子分解……（16）
§ 1.4　完全数、梅审数、费马数……（27）
§ 1.5　高斯函数[x]……（31）
第二章　同余理论……（38）
§ 2.1　同余的概念与基本性质……（38）
§ 2.2　完全剩余系、简化剩余系……（43）
§ 2.3　欧拉函数 $\varphi(m)$……（50）
第三章　不定方程……（56）
§ 3.1　一次不定方程……（56）
§ 3.2　商高不定方程……（62）
§ 3.3　两个平方数的和……（69）
第四章　一元同余方程……（77）
§ 4.1　一次同余方程……（77）
§ 4.2　质数模的高次同余方程……（88）
§ 4.3　合数模的高次同余方程……（93）
第五章　平方剩余与二次同余方程……（100）

§ 5.1　基本性质 …………………………………… (100)
§ 5.2　勒朗德符号 ………………………………… (104)
§ 5.3　亚可比符号 ………………………………… (119)
§ 5.4　质数模的二次同余方程 …………………… (125)
§ 5.5　合数模的二次同余方程 …………………… (134)
第六章　原根与指标 ………………………………… (140)
§ 6.1　阶数 ………………………………………… (140)
§ 6.2　原根存在的必要充分条件 ………………… (144)
§ 6.3　简化剩余系的构造 ………………………… (150)
§ 6.4　指标 ………………………………………… (154)
附　　录：
4000 以下的质数与其最小原根表 ………………… (161)
习题解答 …………………………………………… (164)

第一章　整除性理论

初等整数论的目的是研究整数的性质，而整数的许多性质都要直接或间接地牵涉到整除性，因此我们首先叙述整除性的基本理论，这章主要讨论约数.

§1.1　整除性

我们知道所谓整数指的是…，-2，-1，0，1，2，…，而正整数或者自然数指的是1，2，…. 它们的和、差、积显然都是整数，而两个整数的商就不一定，只有在特殊情况下才是整数.

假如整数 $b(\neq 0)$ 能够整除整数 a，即 $\frac{a}{b}=$ 整数 c，那末 $a=bc$. 这时我们又说 a 是 b 的倍数，b 是 a 的约数或因数. b 能够整除 a，我们用记号 $b\mid a$ 表示，b 不能整除 a 用记号 $b\nmid a$ 表示.

显然　$1\mid a$，$b\mid 0$，$b\mid b$，$b\neq 0$，$b\nmid 1$，$b>1$.

2的倍数我们叫做偶数，不是2的倍数，我们叫做奇数. 当 $a=qb$ 而 $q\neq\pm 1$，$\pm a$ 时，b 叫做 a 的真约数，或真因数.

因为一个非零数的约数的绝对值不大于该数本身的绝对值，所以任一非零数的约数只有有穷个.

由定义我们不难证明下面的定理：

定理 1 假定 $b\neq 0$，$c\neq 0$，我们有

1. 如果 $c\mid b$，$b\mid a$，那末 $c\mid a$；

2. 如果 $b\mid a$，那末 $cb\mid ca$；

3. 如果 $c\mid a$，$c\mid b$，那末 $c\mid(ma+nb)$，这里 m，n 是任意整数；

4. 如果 $b\mid a$，$a\mid b$，那末 $a=b$ 或 $a=-b$

因为 a 与 $|a|$ 有相同的约数，因此我们讨论约数时就可以只就正整数来讨论.

下面是整除的基本定理：

定理 2 对于任意整数 $a,b(\neq 0)$，我们有两个整数 q，r 存在，使

$$a=qb+r,\qquad 0\leqslant r<|b|,$$

并且这 q，r 是唯一的.

证明 因为 a 必在数列

$$\cdots-2|b|,\quad -|b|,\quad 0,\ |b|,\quad 2|b|,\ \cdots$$

中相邻二数之间，我们不妨假定

$$q|b|\leqslant a<(q+1)|b|,$$

于是 $a-q|b|\geqq 0$，$a-q|b|<|b|$，命 $a-q|b|=r$，那末 $0\leqslant r<|b|$，因此当 $b>0$ 时，我们有 $a=qb+r$，当 $b<0$ 时，我们有 $a=(-q)b+r$．这样，我们就证明了 q，r 的存在性，下面我们来证明它们的唯一性.

假如 $a=q_1b+r_1$，$0\leqq r_1<|b|$，那末

$$(q-q_1)b=r_1-r,\qquad 0\leqq|r_1-r|<|b|,$$

即 $|q-q_1||b|<|b|$，因此 $|q-q_1|<1$，但 q,q_1 都是整数，

所以$q=q_1$. 于是$r=r_1$, 这就是说q, r是唯一的，因此定理成立.

譬如$a=13$, $b=5$时，$13=2\cdot5+3$, 这时$q=2$, $r=3$, 又如$a=13$, $b=-5$时，$13=(-2)(-5)+3$, 这时$q=-2$, $r=3$.

上定理2中的r叫做用b除a得到的最小非负余数或简称余数，当$r=0$时，$a=qb$那末a就是b的倍数了.

例 1 试证形如$3n-1$的数不是平方数.

证 我们容易知道任一整数可以写成$3n$或$3n\pm1$, 因为

$$(3n)^2=9n^2=3k,$$

$$(3n\pm1)^2=3(3n^2\pm2n)+1=3k+1,$$

所以$3n-1$不是一个平方数. 因此例成立.

例 2 试证三个相邻数的乘积是3的倍数

证 因为任意数可以写成形如$3n$或$3n\pm1$类型，而同一类型的数相差是3的倍，所以不小于3. 但三个相邻数中任意两数之差小于3，因此三个相邻数分别属上述三类型. 于是其中必有属于$3n$类型的，即3的倍数的，所以例成立.

例 3 假定整数$n>1$, 试证$s=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$不是整数.

证 设k是满足条件$2^k\leqslant n$的最大整数，p是所有不大于n的奇数的乘积，那末在$2^{k-1}ps$的展开式中，除$2^{k-1}p\frac{1}{2^k}$外，其他各项都是整数，所以$2^{k-1}ps$不是整数，即s不是整数，证毕.

我们知道平常所用的数都是十进位的．在日常生活中很多是 12 进位的，譬如一年 12 个月，一英尺是 12 英寸，一天是两个 12 小时，一个圆周角是 30 个 12 度等．现在计算机上用的数是 2，8 及 16 进位的．下面定理是它们的依据．

定理 3 假定 g 是大于 1 的整数，那末任意正整数 a 可以写成

$$a = c_n g^n + \cdots + c_1 g + c_0 \tag{1}$$

这里 $n \geqslant 0$，c_i 是整数，$0 \leqslant c_i < g$，g 叫做 a 的底．

证明 用数学归纳法．当 $a = 1$ 时，$n = 0$，$c_0 = 1$，即 $a = 1$，所以这时 (1) 成立．假定 $0 < a$ 时 (1) 成立，因为 $g > 1$，$a > 0$，所以 a 必定在

$$g^0,\ g^1,\ g^2,\ \cdots,\ g^n,\ \cdots$$

中相邻二数之间，假定

$$g^n \leqslant a < g^{n+1},$$

由定理 2，我们有

$$a = c_n g^n + r, \qquad 0 \leqslant r < g^n,$$

显然 $c_n > 0$ 并且 $c_n < g$．如果 $r = 0$，那末

$$a = c_n g^n + 0 g^{n-1} + \cdots + 0 g + 0,$$

如果 $r \neq 0$，根据归纳法假设

$$r = b_t g^t + \cdots + b_1 g + b_0, \qquad t < n,$$

这里 $0 \leqslant b_i < g$．因此

$$a = c_n g^n + b_t g^t + \cdots + b_1 g + b.$$

于是 (1) 成立，下面证明唯一性．

假定我们又有

$$a = d_m g^m + \cdots + d_1 g + d_0,$$

这里 $m \geqslant 0$，$0 \leqslant d_i < g$，如果 c_i 与 d_i 不完全一致，将上式

与(1)相减得

$$0=e_sg^s+\cdots+e_1g+e_0.$$

这里 s 是 $c_i\neq d_i$ 中 i 的最大数，所以 $e_s\neq 0$. 如果 $s=0$，那末 $e_s=e_0=0$，此不可．如果 $s>0$，那末

$$|e_i|=|c_i-d_i|\leqslant g-1,\ i=0,\ \cdots,\ s-1,$$

并且

$$e_sg^s=-(e_{s-1}g^{s-1}+\cdots+e_0),$$

因此

$$g^s\leqslant|e_sg^s|=|e_{s-1}g^{s-1}+\cdots+e_0|$$
$$\leqslant(g-1)(g^{s-1}+\cdots+g+1)=g^s-1$$

这又不可，所以 c_i 与 d_i 完全一致，即

$$n=m,\ c_i=d_i,\ i=0,\ \cdots,\ n.$$

定理证毕.

譬如 $a=2107$，如果取 $g=10$，显然

$$2107=2(10)^3+(10)^2+7=(2107)_{10}$$

如果取 $g=6$，因为

$$2107=351\times 6+1,\qquad 351=58\times 6+3,$$
$$58=9\times 6+4\qquad 9=6+3.$$

所以

$$2107=1(6)^4+3(6)^3+4(6)^2+3(6)+1,$$

即

$$2107=(13431)_6.$$

习 题 1.1

1．a 的二个倍数的和及差仍然是 a 的倍数.

2．a 的倍数如果不等于零，那末它的绝对值不小于

$|a|$.

3. 整数 a 的个位数如果是 5 的倍数，那末 a 是 5 的倍数.

4. 试证任意奇数的平方减 1 是 8 的倍数.

5. 试证 $3 \mid n(n+1)(2n+1)$，这里 n 是任意整数.

6. 假定 a，b，c，d 都是正整数，并且 $a<b^2$，$a=cd$，$c>b$ 求证 $d<b$.

7. 假如 a 是奇数，那末 $a=4n+1$ 或 $a=4n+3$.

8. 试将数 1112 用底 12 及底 2 表示

9. 假定 d_1，…，d_k 是 n 的全部正约数，试证

$$(d_1 \cdots d_k)^2 = n^k.$$

§1.2 最大公约数、最小公倍数

上节我们是讨论一个数的约数、倍数，这节我们来讨论若干个数的约数、倍数.

假定 c 是 a 的约数，同时又是 b 的约数，即 $c \mid a$，$c \mid b$，那末 c 就叫做 a，b 的**公约数**，因为任一非零数的约数只有有穷个，所以 a，b（a，b 不同时为 0）的公约数也只有有穷个，其中最大的公约数，叫做**最大公约数**，用 (a, b) 来表示，显然 (a, b) 是唯一的，当 $(a, b)=1$ 时，我们叫 a，b **互质**.

譬如 $(12, -18)=6$，$(25, 36)=1$，即 12，-18 的最大公约数是 6，而 25 与 36 互质. 又因为 $(a, 1)=1$，所以 1 与任何数互质.

由定义我们容易得知

$$(a,\ 0)=|a|,\quad (a,\ b)\geqq 1,$$

如果 b 是 a 的倍数，那末 $(a,\ b)=|a|$，再假如

$$a=qb+r,$$

那末

$$(a,\ b)=(b,\ r)$$

这是因为 $(a,\ b)\mid r$，又因为 $(a,\ b)\mid b$，所以 $(a,\ b)\mid (b,\ r)$. 同样，因为 $(b,\ r)\mid a$，$(b,\ r)\mid b$，所以 $(b,\ r)\mid (a,\ b)$，因此上式成立.

任意二个数的最大公约数可以用下面欧几里得(Euclid)算式求得.

假定 a，b 的任意二个整数，由 § 1.1 定理 2，我们有整数 $k\geqslant 1$，使得

$$\begin{array}{ll}
a=q_1b+r_1, & 0<r_1<b,\\
b=q_2r_1+r_2, & 0<r_2<r_1,\\
\cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\\
r_{k-2}=q_kr_{k-1}+r_k, & 0<r_k<r_{k-1},\\
r_{k-1}=q_{k+1}r_k. &
\end{array}\tag{1}$$

由上面第 1 式，我们有 $(a,\ b)=(b,\ r_1)$，因此我们得

$$(a,\ b)=(b,\ r_1)=(r_1,\ r_2)=\cdots=(r_{k-1},\ r_k)=r_k$$

即 r_k 就是所求的 $(a,\ b)$，这就是说求 a，b 的最大公约数可以用欧几里得算法，最后得到的除数 r_k 就是所求的 $(a,\ b)$.

例 1 求 525，231 的最大公约数.

解 由

$$525=2\cdot 231+63$$

$$231=3\cdot 63+42$$

$$63=1\cdot 42+21$$

$$42=2\cdot 21,$$

得

$$(525,\ 231)=21.$$

由上面欧几里得算法，我们还得到下面关于最大公约数的一些基本性质.

定理 1 a, b 的任意公约数是它们的最大公约数 $(a,\ b)$ 的约数.

这是因为如果 $c\mid a$, $c\mid b$, 由(1)显然 $c\mid r_1$, 又因为 $c\mid b$, $c\mid r_1$ 所以 $c\mid r_2$, 这样继续下去，最后我们就得到 $c\mid r_k$, 所以 $c\mid(a,\ b)$.

例 2 试证 $(a,\ b)=(a,\ b+ka)$, 这里 k 是任意整数.

证 设 $(a,\ b)=d$, $(a,\ b+ka)=d'$, 因为 $d\mid a$, $d\mid b$, 所以 $d\mid(b+ka)$, 因此 $d\mid d'$. 同样，$d'\mid d$, 于是例成立.

定理 2 $(a,\ b)c=(ac,\ bc)$, $c>0$

这是因为用 c 乘(1)中各式，那末(1)中 a, b, r_i 就变成 ac, bc, r_ic, 所以 $(ac,\ bc)=(a,\ b)c$.

譬如 $(12,\ -18)=(2,\ -3)6=6$.

定理 3 假定 $(a,\ b)=1$, 那末 $(ac,\ b)=(c,\ b)$.

证明 因为 $(ac,\ b)\mid ac$, $(ac,\ b)\mid bc$ 所以

$$(ac,\ b)\mid(ac,\ bc)=(a,\ b)c=c.$$

再因为 $(ac,\ b)\mid b$, 所以 $(ac,\ b)\mid(c,\ b)$.

又 $(c,\ b)\mid ac$, $(c,\ b)\mid b$, 所以 $(c,\ b)\mid(ac,\ b)$, 于是 $(ac,\ b)=(c,\ b)$, 因此定理成立.

譬如 $(300,\ -18)=(12\cdot 25,\ -18)=(12,\ -18)=6$.

由上定理我们很容易得出下面几个常用的结果.

当 $b\mid ac$ 时，如果 $(a,\ b)=1$, 我们就有 $b\mid c$, 这是因为

$(ac, b)=b$，再由上定理 $(ac, b)=(c, b)$，所以 $(c, b)=b$，因此 $b|c$.

又当 $a|c$，$b|c$ 时，如果 $(a, b)=1$，我们有 $ab|c$，这是因为从 $a|c$ 得 $c=ac_1$，所以 $b|ac_1$，因此 $b|c_1$，于是 $ab|ac_1$，即 $ab|c$.

又当 $(a, c)=1$，$(b, c)=1$ 时，我们有 $(ab, c)=1$，这是因为由上定理，$(ab, c)=(b, c)=1$.

再如果 $(a, b)=1$，那末 $(ab, a+b)=1$，这是因为由 $(a, a+b)=1$，$(b, a+b)=1$，我们有 $(ab, a+b)=1$.

定理 4 假定 $c(>0)$ 是整数 a，b 的公约数，那末

$$\left(\frac{a}{c}, \frac{b}{c}\right)=\frac{(a, b)}{c}$$

证明 因为

$$\left(\frac{a}{c}, \frac{b}{c}\right)c=\left(\frac{a}{c}\cdot c, \frac{b}{c}\cdot c\right)=(a, b),$$

所以定理成立.

特别，假如 $c=(a, b)=d$，那末 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$，反过来，如果 $\left(\frac{a}{c}, \frac{b}{c}\right)=1$，那末 $c=(a, b)$，这就是下定理：

定理 5 假定 $c>0$，那末 $\left(\frac{a}{c}, \frac{b}{c}\right)=1$ 的必要充分条件是 $c=(a, b)$.

从欧几里得算法倒推，我们容易得到下面重要定理：

定理 6 假定 $(a, b)=d$，那末有整数 x，y 存在，使

$$ax+by=d.$$

譬如由例 1，我们有

$$21=63-1\cdot 42=63-1\cdot(231-3\cdot 63)$$
$$=4\cdot 63-1\cdot 231=4(525-2\cdot 231)-1\cdot 231$$
$$=4\cdot 525-9\cdot 231.$$

即
$$525\cdot 4+231(-9)=21.$$

当$(a,b)=1$时，我们有$ax+by=1$，反过来也成立，于是$(a,b)=1$的必要充分条件是有整数x，y使$ax+by=1$成立。

譬如　$14\cdot 2+9(-3)=1$，所以$(14,9)=1$。

例 3　假定$a>1$，m，n是正整数，试证
$$(a^m-1,\ a^n-1)=a^{(m,n)}-1.$$

证　当$m=n$时，等式显然成立，假定$m>n$，$m=qn+r$，于是
$$a^m-1=(a^n-1)a^{m-n}+a^{m-n}-1$$
$$=(a^n-1)a^{m-n}+(a^n-1)a^{m-2n}+a^{m-2n}-1$$
$$=(a^n-1)(a^{m-n}+a^{m-2n}+\cdots+a^{m-qn})+a^r-1$$

因此
$$(a^m-1,\ a^n-1)=(a^n-1,\ a^r-1)=(a^r-1,\ a^{r_1}-1)=\cdots$$
$$=(a^d-1,\ a^0-1)=a^d-1.$$

这里$d=(m,n)$，所以例成立。

上面是介绍二个整数的最大公约，任意多个数的最大公约也是这样。

一般n个数a_1，a_2，…，a_n只要它们不同时为零，它们的最大公约数也是唯一存在的，我们用$(a_1,\cdots,a_n)$表示。当$(a_1,\cdots,a_n)=1$时，我们就说a_1，…，a_n**互质**，假如a_1，…，a_n中任意二个数都是互质的，我们就说a_1，…，a_n**两两互质**，我们容易看到a_1，…，a_n如果两两互质，当然a_1，

$\cdots$, a_n 互质，但 a_1, $\cdots$, a_n 互质却不一定两两互质.

譬如 $(6, 10, 15)=1$，即 6, 10, 15 互质，但它们不是两两互质.

再无穷多个数 a_1, $\cdots$, a_n, $\cdots$同样也有最大公约数$(a_1, \cdots, a_n, \cdots)$.

求三个数 a, b, c 的最大公约数 (a, b, c)，我们可以根据

$$(a, b, c)=((a, b), c) \tag{2}$$

求得，这就是说先求出 a, b 的最大公约数 (a, b)，再求出 (a, b), c 的最大公约数$((a, b), c)$就得到所求的 (a, b, c) 了.

(2) 式的证明如下：

假定$(a, b, c)=d_1$, $((a, b), c)=d_2$, 因为 d_2 是(a, b), c 的公约数，而 (a, b) 又是 a, b 的公约数，所以 d_2 是 a, b, c 的公约数，因此 $d_2 \leqq d_1$, 再因为 d_1 是 a, b, c 的公约数，所以应该是(a, b), c 的公约数，因此 d_1 是$((a, b), c)$的约数，即 $d_1 \leqq d_2$, 于是 $d_1=d_2$ 所以(2)式成立

根据定理 6 我们很容易把(a, b, c)写成

$$(a, b, c)=ax+by+cz,$$

这里 x, y, z 都是整数.

一般对于 n 个数 a_1, $\cdots$, a_n 的最大公约数也是如此. 假如$(a_1, a_2)=d_2$, $(d_2, a_3)=d_3$, $\cdots$, $(d_{n-1}, a_n)=d_n$, 那末

$$(a_1, a_2, \cdots, a_n)=d_n,$$

并且$(a_1, \cdots, a_n)$也可以写成

$$(a_1, \cdots, a_n)=a_1x_1+\cdots+a_nx_n,$$

这里 x_1, $\cdots$, x_n 都是整数. 即对于 n 个数定理 6 同样成立.

定理5对于n个数显然成立.

例 4 求$(136, 221, 391)$.

解
$$(136, 221, 391)=(136, (221, 391))=(136, 17)=17.$$

我们也可以这样做:

$$\begin{aligned}(136, 221, 391)&=(136, 221-136, 391-2\cdot 136)\\&=(136, 85, 119)=(51, 85, 34)\\&=(17, 17, 34)=17.\end{aligned}$$

又因为$5\cdot 136-3\cdot 221=17$, $(-22)\cdot 17+1\cdot 391=17$, 所以

$$(-110)\cdot 136+66\cdot 221+1\cdot 391=17.$$

上面介绍了最大公约数, 下面我们来讨论最小公倍数.

假定$m\neq 0$是a的倍数, 同时又是b的倍数, 那末m就叫做a, b的**公倍数**, 在a, b的公倍数中显然不存在最大数, 但有唯一的最小正公倍数, 我们叫它做a, b的**最小公倍数**, 用$[a, b]$来表示.

最小公倍数与公倍数之间也有与最大公约数与公约数之间类似的重要关系.

定理 7 a, b的公倍数是它们的最小公倍数$[a, b]$的倍数.

证明 假定k是a, b的公倍数, 用$[a, b]=m$除k得

$$k=qm+r, \quad 0\leq r<m,$$

因为$a|k$, $a|m$, 所以$a|r$. 同样$b|r$, 于是r是a, b的公倍数, 但m是a, b的最小公倍数, 所以$r=0$, 这就是说$k=qm$即k是m的倍数, 因此定理成立.

下面是最大公约数与最小公倍数间一个重要关系.

定理 8 假如 $ab>0$，那末

$$[a, b](a, b)=ab.$$

证明 假定 $[a, b]=m$，$(a, b)=d$，因为 $a\mid m$，$b\mid m$，所以 $ab\mid ma$，$ab\mid mb$，因此 $ab\mid(ma, mb)$，即 $ab\mid md$.

又因为 $a\left|\frac{ab}{d}\right.$，$b\left|\frac{ab}{d}\right.$，即 $\frac{ab}{d}$ 是 a, b 的公倍数，由定理 7，$m\left|\frac{ab}{d}\right.$，于是 $md\mid ab$，因此 $ab=md$，所以定理得证.

譬如 $[6, 9]=18$，$(6, 9)=3$，这时 $18\times3=6\times9$.

特别，当 $(a, b)=1$ 时，我们就有 $[a, b]=ab$，即这时 ab 是 a，b 的最小公倍数，反过来，假如 a，b 的最小公倍数是 ab，那末 $(a, b)=1$，因此 $(a, b)=1$ 的必要充分条件是 $[a, b]=ab$.

下面是与定理 4 类似的定理.

定理 9 假定 $k(>0)$ 是整数 a，b 的公倍数，那末

$$\left(\frac{k}{a}, \frac{k}{b}\right)=\frac{k}{[a, b]}.$$

证明 因为

$$\left(\frac{k}{a}, \frac{k}{b}\right)ab=(kb, ka)=k(a, b),$$

再由定理 8 即得所求式. 证毕.

特别，当 $k=[a, b]=m$ 时，那末 $\left(\frac{m}{a}, \frac{m}{b}\right)=1$，反过来，如果 $\left(\frac{k}{a}, \frac{k}{b}\right)=1$，那末 $k=[a, b]$. 这就是下定理：

定理 10 假定 $k>0$，那末 $\left(\frac{k}{a}, \frac{k}{b}\right)=1$ 的必要充分条

件是 $k=[a, b]$.

最后我们来讨论最小公倍数的求法.

由定理 8，我们有

$$[a, b]=\frac{ab}{(a,b)},$$

因此我们先求出 (a, b)，再根据这公式立即求得 $[a, b]$.

譬如 $[525, 231]=\frac{525\cdot 231}{21}=25\cdot 231=5775.$

例 5 设 a, b 是非零整数，试证有 4 个整数 h, k, r, s 存在使

$$hs-kr=1, \quad ak+hs=0$$

证 假定 a, b 都是正数. 因为 $[a, b](a, b)=ab$，设 $[a, b]=ak$，$s=-a/(a, b)$，即得 $ak+bs=0$. 再因为

$$k=ab/a(a, b)=b/(a, b),$$

所以 $(k, s)=1$，因此有 $hs+(-k)r=1$，于是例成立.

一般 n 个数 a_1, …, a_n 的最小公倍数 $[a_1, \cdots, a_n]$ 也是唯一的. 同定理 7 一样，a_1, …, a_n 的公倍数是它的最小公倍数 $[a_1, \cdots, a_n]$ 的倍数. 三个数 a, b, c 的最小公倍数 $[a, b, c]$，我们可以根据

$$[a, b, c]=[[a, b], c] \tag{3}$$

求出，这就是说我们先求出 a, b 的最小公倍 $[a, b]$，再求出 $[a, b]$, c 的最小公倍数 $[[a, b], c]$，就是所求的 $[a, b, c]$.

(3) 式可与 (1) 类似地证明如下：

假定 $[a, b, c]=m_1$，$[[a, b], c]=m_2$，因为 m_1 是 $[a, b]$, c 的公倍数，而 $[a, b]$ 又是 a, b 的公倍数，所以 m_1 是 a, b, c 的公倍数，因此 $m_2 \geq m_1$. 再因为 m_1 是 a, b, c 的公倍

数，所以又是$[a, b]$，c的公倍数，因此$m_1 \geq m_2$，于是$m_1 = m_2$，所以(3)成立．

一般n个数a_1，…，a_n的最小公倍数也是如此，假如$[a_1, a_2] = m_2$，$[m_2, a_3] = m_3$，…，$[m_{n-1}, a_n] = m_n$，那末

$$[a_1, a_2, \cdots, a_n] = m_n$$

假如a，…，a_n两两互质，那末

$$[a_1, a_2, \cdots, a_n] = a_1 a_2 \cdots a_n.$$

譬如

$$\begin{aligned}[136, 221, 391] &= [[126, 221], 391] \\ &= \left[\frac{136 \cdot 221}{17}, 391\right] = [1768, 391] \\ &= \frac{1768 \cdot 391}{17} = 104 \cdot 391 = 40664.\end{aligned}$$

要注意的是对于两个以上的数，定理7显然成立，定理9也成立，但定理8不成立，譬如$(6, 18, 4) = 2$，$[6, 18, 4] = 36$．但$6 \cdot 18 \cdot 4 = 432$．

习　题　1.2

1．求　$(24871, 3468)$，$(120, 504, 882)$，
$[135, 513, 3114]$．

2．假定n是大于1的奇数，试证$n^3 - n$是24的倍数．

3．假如$ax + by = c$，试证$(a, b) \mid c$．

4．试证a_1，…，a_n，…的公约数是它们的最大公约数的约数．

5．假如a_1，a_2，…，a_k是两两互质的正数，试证

$$[a_1, a_2, \cdots, a_k] = a_1 a_2 \cdots a_k.$$

6．假如$[a, b] = m$，那末$(a + b, m) = (a, b)$．

7. 试证在数列a，$2a$，$3a$，…，ba中，b的倍数的个数等于(a, b).

8. 求所有满足$(x, y)=8$，$[x, y]=64$的整数x，y.

9. 试证$(a^n, b^n)=(a, b)^n$，$[a^n, b^n]=[a, b]^n$

10. 假如$(b, c)=1$，那末$(a, bc)=(a, b)(a, c)$.

11. 求证$(a, b, c)(ab, bc, ca)=(a, b)(b, c)(c, a)$.

12. 假如$(a, b)=1$，那末$(a-b, a+b)=1$或2.

13. 假如$a_1b_2-a_2b_1=\pm1$，那末分数$\frac{a_1+a_2}{b_1+b_2}$不能简化.

14. 假定$(a, b)=d$，试证d是所有形状象$f(x, y)=ax+by$的整数中的最小正数，即$d=ax_0+by_0$，这里x，y是任意整数.

§1.3 质数、整数的质因子分解

在正整数1，2，3，4，…中，我们可以看到有些数只有二个正约数，有些数有二个以上的正约数，只有1是例外，它只有一个正约数，也就是说它只能用自身除尽.

大于1的整数，如果它的正约数只有1及它自身，我们就叫它做质数. 否则，也就是说，除1及它自身外还有其他正约数的正数，我们叫它做合数. 因此1既不是质数，也不是合数，它在正整数中非常特殊.

譬如，2，3，5，7，11，… 等都是质数，而4，6，8，9，10，…等都是合数，偶数中只有2是质数，其余都是合数.

下面我们所说的数都是大于1的正整数：

任意数 a 的最小约数 $q(>1)$ 是质数，因为如果 q 不是质数，那末它就有约数 q_1， $1<q_1<q$， 显然 q_1 又是 a 的约数，这与 q 是 a 的最小约数的假设不合，因此 q 是质数．于是任意数 a 最少有一个质约数，这是因为如果 a 不是质数，那末它的最小的正约数就是它的质约数．

定理 1 假定 a 是合数，q 是它的最小正约数，那末

$$q\leqq\sqrt{a}.$$

证明 因为 q 是 a 的约数，即 $q\mid a$，所以我们有 $a=qa_1$，显然这里 $a_1\geqq q$，于是 $a\geqq q^2$，这就是说 $q\leqq\sqrt{a}$，因此定理成立．

例 1 假定 n 是合数，试证 n 位数 $\underbrace{11\cdots11}_{n\text{个}}$ 也是合数．

证 设 $n=ab$，那末

$$10^n-1=(10^a)^b-1=(10^a-1)\ (10^{a(b-1)}+\cdots+10^a+1),$$

即

$$9(\underbrace{11\cdots11}_{n\text{个}})=9(\underbrace{11\cdots11}_{a\text{个}})(10^{a(b-1)}+\cdots+10^a+1),$$

所以

$$\underbrace{11\cdots11}_{n\text{个}}=\underbrace{11\cdots11}_{a\text{个}}(10^{a(b-1)}+\cdots+10^a+1).$$

因此例成立．

要注意的是这例的逆不成立，譬如 3 是质数，但 $111=3\cdot37$ 是合数．

合数显然有无穷多个，譬如偶数以及任意数 m 的倍数都有无穷个．此外我们还有：

定理 2 对于任意数 $n(>1)$ 有 n 个相邻的合数．

证明 因为 n 个数

$$(n+1)!+2,\ (n+1)!+3,\ \cdots,\ (n+1)!+n+1$$

都是合数，所以定理成立.

譬如 $n=4$ 时，122，123，124，125 是 4 个相邻的合数，当然 24，25，26，27 也是 4 个相邻的合数，相邻的质数除 2，3 外显然不存在．但我们有：

定理 3 质数有无穷多个.

证明 假定 p 是任一质数，q 是 $a=p!+1$ 的质约数，因为 $q\nmid p!$，所以 $q>p$，这就是说对任意给出的质数还有比它大的质数，因此质数的个数是无穷，于是定理成立.

同样我们还有下面更广泛的结果：

定理 4 形状象 $4n-1$ 的质数有无穷多个.

证明 假定 $4n_1-1$，$4n_2-1$，$\cdots$，$4n_k-1$ 是不大于 $4n-1$ 而形状与它一致的所有质数，同定理 3 的证明一样，

$$a=4(4n_1-1)(4n_2-1)\cdots(4n_k-1)-1$$

有不同于 $4n_i-1$，$i=1$，$\cdots$，k，的质因数，显然 a 的质因数是奇数，但奇数可以写成 $4n+1$ 或 $4n-1$，而

$$(4l+1)(4m+1)=4(4lm+l+m)+1$$

所以 a 的质因数中不能都是 $4n+1$ 形状的，其中必有形如 $4n-1$ 的，因此定理成立.

同样，形如 $4n+1$ 的质数也有无穷多个.

1837 年狄利克雷(G.L. *Dirichlet*，1805～1859)证明：假如 $(a,\ d)=1$，那末形状象 $p=a+dt$，t 是正整数的质数有无穷多个，也就是说，在以 a 为首项，d 为公差的算术级数中有无穷多个质数，这就是著名的狄利克雷的算术级数的质数定理.

又不大于正整数 $n(>1)$ 的质数的个数通常用 $\pi(n)$ 表示，譬如 $\pi(3)=2$，$\pi(10)=4$，$\pi(100)=25$，$\pi(1000)=168$，它没有一个精确的表达式，但当 n 非常大时，$\pi(n)$ 与 $\frac{n}{\log n}$ 近似，确切地说就是

$$\lim_{n\to\infty}\frac{\pi(n)}{\frac{n}{\log n}}=1,$$

这就是著名的质数定理，这定理大约是在 1793 年高斯(C.F. Gauss，1777～1855) 与勒朗德(A. M. Legendre，1752～1833)作为猜想提出的．一百年后，1896 年才由法国数学家哈达马(J. Hadamard，1865～1963)及德拉威力伯桑 (C. de la vallée Poussin，1866～1962)同时独立地证明，1948 年挪威数学家宰尔伯格 (A. selbarg) 与匈牙利数学家爱推斯 (P. Erdos) 另有初等证明，就是这个所谓的初等证明，在这里我们也是无法介绍的．

一个数是否是质数，我们还没有一般方法来判别，主要原因是质数在正整数中分布的情况很不规则，有些问题到现在还没有得到解决．譬如：

高斯曾发现在第 26379 个一百中没有质数，但在第 27050 个一百中却有 17 个质数，比在第 3 个一百中还多一个．1846 年白特朗(Bertrand) 曾推测当 $2a>7$时，a 与 $2a-2$ 之间至少有一个质数，切比雪夫(П. А. чебышев，1821～1894)在 1852 年证明了这个猜测．杰波夫(Desloves) 猜测在 n^2 与 $(n+1)^2$ 之间至少有二个质数．

再如

3，5；5，7；11，13；17，19；29，31；

41，43；…；10016957，10016959；…

等等，相邻的两个奇数同时为质数，这样的数叫做孪质数。孪质数是否有无穷多个？目前我们知道的最大孪质数是：

$$297\cdot 2^{546}-1,\ 297\cdot 2^{546}+1$$

上面孪质数是其差为2的质数对，同样其差为6的质数对有：

5，11；7，13；11，17；13，19；17，23；23，29；

31，37；37，43；41，47；47，53；53，59，61，67；

…

是否有无数对？

又如

$4=2+2$，$6=3+3$，$8=3+5$，$10=5+5$，$12=5+7$，

$14=7+7$，$16=5+11$，$18=5+13$，$20=7+13$，…

等等，2以上的偶数是否都可以写成两个质数的和，这是1742年古特拔黑(C. Goldbach，1690～1764)提出的猜测，是数学史上有名的古特拔黑问题，也是数论上悬而未决的问题，1966年陈景润证明了，所有偶数（充分大）是一个质数与另一数的和，后者或是质数，或仅仅是两个质数的乘积。

对一个给出的数我们可以用下面方法求出所有不大于它的质数，因而也就判别了它是否是质数。

假定a是任一数，我们先把所有不超过a的正数依大、小顺序写出：

1，2，3，4，5，6，7，……，a

再把1划去，剩下来的第一个数是2，因为它没有小于自身的约数，所以它是质数．又从2起划去所有2的倍数，剩下

来的第一个数是3，它不是2的倍数，所以它是质数．这样继续下去，当我们把所有小于$\sqrt{a}$的质数的倍数划去后，剩下来的数就是所有不大于a的质数，这是因为根据定理1，任意小于a的合数都有小于$\sqrt{a}$的质因数，当我们划去所有小于$\sqrt{a}$的质数的倍数时，它已被划去不复存在了．这就是所谓的爱拉托散（Eratosthenes，约274～194 B.C.）的筛子法，这种方法逐步把质数求出来，好象是用筛子从整数中把质数筛出来一样，它是希腊时代爱拉托散发明的．

譬如$a=30$，这时$\sqrt{a}<6$，在

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,$$
$$11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 20,$$
$$21,\ 22,\ 23,\ 24,\ 25,\ 26,\ 27,\ 28,\ 29,\ 30,$$

中我们把所有不大于6的质数的倍数划去，剩下来的数

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

就是所有不大于30的质数．

这个方法虽然简单，但当a较大时，计算非常冗长，因而很不实用，但是舍此外，目前还没有较好方法．

下面是质数的一个基本性质．

定理 5 假如p是质数，$p\mid ab$，那末$p\mid a$或$p\mid b$．

证明 假如$p\nmid a$，那末$(a,\ p)=1$，因此由§1.2定理3后面结论，我们即得$p\mid b$，所以定理成立．

于是我们不难推得假如质数$p\mid p_1p_2\cdots p_n$，这里p_i都是质数，那末p必定能够除尽某个p_k，即$p\mid p_k$，又因为p_k是质数，所以$p=p_k$，这就是说假如$p\mid p_1p_2\cdots p_n$，那末$p=p_k$．

以上定理非常重要，很多方面都需要它．

例 2 假定p是质数，试证满足

$$a^2 = pb^2$$

的正整数 a，b 不存在.

证 我们用反证法，假定有两正整数 a，b 使

$$a^2 = pb^2$$

成立，命 $d=(a, b)$，即 $a=da_1$，$b=db_1$，$(a_1, b_1)=1$，代入上式消去 d^2 得

$$a_1^2 = pb_1^2,$$

于是 $p\mid a_1^2$，所以 $p\mid a_1$，设 $a_1=pa_2$，我们有

$$a_2^2 p = b_1^2,$$

显然 $p\mid b_1$，因此 p 是 a_1，b_1 的公约数，这与 $(a_1, b_1)=1$ 矛盾，所以例成立.

下面是整数的**算术基本定理**，由这也可以看出质数在整除性理论中所起的作用.

定理 6 凡大于 1 的正整数，除因数的顺序外，能够唯一的分解为质因数的乘积，即任意正数

$$a = p_1p_2\cdots p_r,\quad p_i \text{ 是质数}, \tag{1}$$

如果 $$a = q_1q_2\cdots q_s,\quad q_i \text{ 是质数},$$

那末 $r=s$，并且 p_1，p_2，$\cdots$，p_r 除顺序外与 q_1，$q_2\cdots$，q_s 一致.

证明 假如 a 是质数，(1)显然成立. 假如 a 是合数，p_1 是它的最小正约数，因此 p_1 是质数，这时我们有 $a=p_1a_1$，如果 a_1 是质数，那末(1)即告成立. 如果 a_1 是合数，p_2是它的最小质约数，那末 $a_1=p_2a_2$，于是我们有 $a=p_1p_2a_2$，这样继续进行，因为 $a>a_1>a_2>\cdots$，所以经过有限回后必得到 $a=p_1p_2\cdots p_r$，这里 p_i 都是质数，因此(1)成立，即分解的可能性成立.

下面对 r 用数学归纳法来证明分解的唯一性.

当 $r=1$ 时，$p_1=q_1\cdots q_s$，因为 p_1 是质数，所以 $s=1$，因此 $p_1=q_1$，这就是说当 $r=1$ 时分解的唯一性成立. 假定 $r-1$ 时唯一性成立. 因为

$$p_1p_2\cdots p_r=q_1q_2\cdots q_s,$$

这式左边能够用 p_1 整除，当然右边也能够用 p_1 整除，由上面定理 5 后面的结论，我们得知 p_1 能够整除 q_1，q_2，$\cdots$，q_r 中某一数，假定 $p_1|q_1$，因而 $p_1=q_1$，从上式两边消去 p_1，我们就有

$$p_2\cdots p_r=q_2\cdots q_s$$

根据归纳法假设得 $r-1=s-1$，并且适当调换顺序可以使 $p_i=q_i$，$i=2$，$\cdots$，r. 于是 $r=s$ 并且 $p_i=q_i$，$i=1$，2，$\cdots$，r.

所以分解的唯一性成立.

定理证毕.

假如把(1)中相同质数集中，我们就得到

$$a=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},$$

p_1，$\cdots$，p_k 是互异质数，这个式叫做 a 的标准分解式或标准表示式，其中 a_i 是 p_i 在 a 的最高幂，我们又常用 $p_i(a)$ 表示，即 $a_i=p_i(a)$.

譬如 $5775=3\cdot5^2\cdot7\cdot11$，$40664=2^3\cdot13\cdot17\cdot23$.

利用标准分解式，我们可以得到下面关于约数的一些基本性质.

我们不难得知，d 是 a 的正约数的必要充分条件是

$$d=p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k},$$

$$0\leqslant d_i\leqslant a_i,$$

这样一切可能的数就是 a 的所有正约数，于是 a 的正约数的个数

$$T(a)=(a_1+1)(a_2+1)\cdots(a_k+1)=\prod_{i=1}^{k}(a_i+1),$$

a 的所有正约数的和

$$S(a)=\sum_{i_1=0}^{a_1}\cdots\sum_{i_k=0}^{a_k}p_1^{i_1}\cdots p_k^{i_k}=\sum_{i_1=0}^{a_1}p_1^{i_1}\cdots\sum_{i_k=0}^{a_k}p_k^{i_k}$$

$$=\frac{p_1^{a_1+1}-1}{p_1-1}\cdots\frac{p_k^{a_k+1}-1}{p_k-1}=\prod_{i=1}^{k}\frac{p_i^{a_i+1}-1}{p_i-1}$$

这里我们引用了等比数列求和公式，

假如 a_1，$\cdots$，$a_{T(a)}$ 是 a 的所有正约数，命 $a=a_ia_i'$，那末 a_1'，$\cdots$，$a_{T(a)}'$ 显然也是 a 的所有正约数，于是 a 的所有正约数的乘积

$$P(a)=a_1a_2\cdots a_{T(a)}=\sqrt{(a_1a_1')(a_2a_2')\cdots(a_{T(a)}a_{T(a)}')}$$

$$=\sqrt{\underbrace{a\cdots a}_{T(a)\text{个}}}=a^{\frac{1}{2}T(a)}$$

譬如 $a=60=2^2\cdot3\cdot5$，这时

$$T(a)=(2+1)(1+1)(1+1)=3\cdot2\cdot2=12,$$

$$S(a)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=7\cdot4\cdot6=168,$$

$$P(a)=60^6=46656000000,$$

实际上 60 的正约数是

1，2，3，4，5，6，10，12，15，20，30，60，

读者试以此验证上面的结果.

再利用标准分解式我们也很容易求出若干个数的最大公

约数及最小公倍数.

假定

$$a=p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m},\quad b=p_1^{b_1}p_2^{b_2}\cdots p_m^{b_m},$$

这里 a_i，b_i 都是正整数，其中有的可能为 o，那末

$$(a,\ b)=p_1^{c_1}p_2^{c_2}\cdots p_m^{c_m},\quad [a,\ b]=p_1^{d_1}p_2^{d_2}\cdots p_m^{d_m}$$

这里 c_i 是 a_i，b_i 中较小的数，d_i 是 a_i，b_i 中较大的数，即

$$c_i=min(a_i,\ b_i),\quad d_i=max(a_i,\ b_i).$$

譬如 $a=136=2^3\cdot17$，$b=221=13\cdot17$，$c=391=17\cdot23$，于是 $(a,\ b,\ c)=17$，$[a,\ b,\ c]=2^3\cdot13\cdot17\cdot23=40664$，这结果与前面求得的一致.

当 a，b 互质，即 $(a,\ b)=1$ 时，我们命

$$a=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r},\quad b=q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s},\quad a_i,\ b_i>o$$

这里 p_1，…，p_r，q_1，…，q_s 是互异的质数，于是

$$ab=p_1^{a_1}\cdots p_r^{a_r}\cdot q^{b_1}\cdots p_s^{b_s}$$

是 ab 的标准分解式，因此我们有

$$T(ab)=T(a)\cdot T(b),\quad S(ab)=S(a)\cdot S(b)$$

并且 $P(ab)=(ab)^{\frac{1}{2}T(ab)}=(ab)^{\frac{1}{2}T(a)T(b)}$

$$=P(a)^{T(b)}\cdot P(b)^{T(a)}.$$

要注意的是当 $(a,\ b)\neq1$ 时，上面三个公式是不成立的. 譬如 $a=525=3\cdot5^2\cdot7$，$b=231=3\cdot7\cdot11$，于是 $ab=3^2\cdot5^2\cdot7^2\cdot11$，所以 $T(ab)=54$，$S(ab)=275652$，显然 $T(ab)\neq T(a)T(b)$. $S(ab)\neq S(a)S(b)$. 因此 $P(ab)\neq P(a)^{T(b)}\cdot P(b)^{T(a)}$.

例 3 假定整数 $a>2$，试证 $S(a)\leqslant a\sqrt{a}$.

证 假如 $a=2^k$，$k\geqslant2$，那末

$$S(a)=2^{k+1}-1<2^{k+1}=a\cdot2\leqslant a\cdot2^{\frac{k}{2}}=a\sqrt{a}.$$

假如 $a=p^k$，p 是奇质数，那末

$$S(a)=\frac{p^{k+1}-1}{p-1}=\frac{p^k-\frac{1}{p}}{1-\frac{1}{p}}<\frac{a}{1-\frac{1}{p}}$$

$$=a\cdot\frac{1}{1-\frac{1}{p}}\leqslant a\frac{1}{1-\frac{1}{3}}$$

$$=a\frac{3}{2}<a\sqrt{3}\leqslant a\sqrt{a}.$$

一般假如 $a=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$，于是

$$S(a)=S(2^{\alpha_0})S(p_1^{\alpha_1})\cdots S(p_r^{\alpha_r})$$

$$\leqslant 2^{\alpha_0}\sqrt{2^{\alpha_0}}\,p_1^{\alpha_1}\sqrt{p_1^{\alpha_1}}\cdots p_r^{\alpha_r}\sqrt{p_r^{\alpha_r}}=a\sqrt{a}.$$

证毕.

习 题 1.3

1. 试求 2160 的正约数的个数及其和.

2. 试证 $pC_r=\dfrac{p(p-1)\cdots(p-r+1)}{r!}$ 能够用 p 整除，这里 p 是大于 r 的质数.

3. 假如 $x^2+y^2=axy$ 有正整数解，试求 a.

4. 假如 $3\mid(a^2+b^2)$，那末 $3\mid a$，$3\mid b$.

5. 求只有 10 个正约数的最小正数.

6. 求所有正约数的和等于 15 的最小正数.

7. 求所有正约数的积等于 64 的一切正整数.

8. 证明一个正整数等于它的所有正约数（除该数自身外）的积的必要充分条件是这正整数是一个质数的立方或是两个不同质数的乘积.

9. 假定a, b, c是任意整数，求证

$\max(\min(a, b), \min(a, c)) = \min(a, \max(b, c))$

10. 试用标准式证明$[(a, b), (a, c)] = (a, [b, c])$.

11. 试证对于任意正整数k，不论多大，总有无穷多个数a，使得

$$a+1, \cdots, a+k-1$$

中没有一个质数.

12. 假定$n>2$，试证n与$n!$之间至少有一个质数.

13. 试证形如$3n+2$的质数有无穷多个.

14. 一个数从左向右读与从右向左读得出同一数，叫做回文数，譬如12321，1234321都是回文数.

1）两位数的回文数有多少个？

2）三位数的回文数有多少个？

3）n位数的回文数有多少个？

§1.4 完全数、梅审数、费马数

上节我们介绍了正整数a的所有正约数和$S(a)$的公式，因为a的约数包括1及它自身，所以当$a>1$时，$S(a)\geqq a+1$. 假如$S(a)=a+1$，那末a就是质数了，假如$S(a)=2a$，我们就叫a做**完全数**.

譬如　$6=1+2+3$，$28=1+2+4+7+14$，

所以6，28都是完全数.

下面我们来考虑完全数究竟是那一种形状的数？

假定a是偶完全数，命

$$a=2^n k,\ n\geqslant 1,\ (2, k)=1,$$

因为

$$S(a)=S(2^n)S(k)=(2^{n+1}-1)S(k),$$
$$S(a)=2a=2^{n+1}k,$$

所以

$$S(k)=\frac{2^{n+1}k}{2^{n+1}-1}=k+\frac{k}{2^{n+1}-1}$$

因为 $S(k)$ 是整数，所以 $\frac{k}{2^{n+1}-1}$ 也是整数，因此它是 k 的约数，但 $S(k)$ 是 k 的所有约数的和，所以 k 只有二个约数，一个是 k 自身，另一个是 $\frac{k}{2^{n+1}-1}$，因此 k 是质数，并且 $\frac{k}{2^{n+1}-1}=1$，即 $k=2^{n+1}-1$，于是 $a=2^n(2^{n+1}-1)$.

反过来，假如 $a=2^n(2^{n+1}-1)$，$k=2^{n+1}-1$ 是质数，那末

$$S(a)=S(2^nk)=S(2^n)S(k)=(2^{n+1}-1)(k+1)$$
$$=(2^{n+1}-1)2^{n+1}=2a.$$

因此 a 是完全数，于是我们有：

定理 1 正整数 a 是偶完全数的必要充分条件是

$$a=2^n(2^{n+1}-1),\quad n\geqq 1,$$

并且 $2^{n+1}-1$ 是质数.

于是求偶完全数的问题就归结于求形状是 2^m-1 的质数的问题，但是 m 要满足什么条件，2^m-1 才是质数呢?

定理 2 假如 2^m-1 是质数，那末 m 是质数.

证明 我们用反证法来证明. 假如 m 是合数，$m=qt$，那末

$$2^m-1=(2^t)^q-1=(2^t-1)(2^{t(q-1)}+\cdots+1),$$

但 $1<2^r-1<2^m-1$，这与 2^m-1 是质数的假设不合，所以 m 应该是质数，因此定理成立．

要注意的是上定理的逆是不成立的，也就是说当 p 是质数时，2^p-1 不一定是质数，譬如 $2^{11}-1=2047=23\times 89$.

当 p 是质数时，形状象 2^p-1 的数叫做梅审(M，Mers-snne，1588～1648))数，用 M_p 表示，即

$$M_p=2^p-1,$$

因此，梅审数有的是质数，有的是合数，迄今知道是质数的，只有：

$p=2$，3，5，7，13，17，19，31，61，89，107，127，521，607，1279，2203，2281，3217，4253，4423，9689，9941，11213，19937，21701，23209，44497

时的 27 个，从第 13 个梅审数起都是 1952 年以后借助电子计算机陆续发现的．第 27 个梅审数是 1979 年得到的，它是 13395 位①的非常大的数．

于是定理 1 可改写为 a 是偶完全数的必要充分条件是

$$a=\frac{1}{2}M_p(M_p+1),$$

并且 M_p 是质数．因此偶完全数由质梅审数唯一决定，所以，偶完全数迄今知道的也只有 27 个．再直到现在还没有出现一个奇完全数，奇完全数是否存在也是数论中没有解决的难题．奇完全数也许有，现在只知道如果有，它必大于 10^{120}，并且至少有 8 个不同的质因数．

一个正整数 a 如果它的所有正约数的和是 a 的 k 倍，即

① 如果用 4 位对数表，则只能得 13394 位．

$S(a)=ka$，那末 a 叫做 k **重完全数**．第1个3重完全数是120，欧拉找出的第2个是672，第3个是523776．第一个4重完全数是30240．这种重完全数现在时有出现．

与梅审数形状类似的是 2^m+1 形状的数，它是质数时，m 应该具备什么条件？

定理 3 假如 2^m+1 是质数，那末 m 是2的幂，即

$$m=2^k.$$

证明 假如 m 有奇约数 q，$m=qr$，那末

$$2^m+1=(2^r)^q+1=(2^r+1)(2^{r(q-1)}-\cdots+1),$$

但 $1<2^r+1<2^m+1$，这与 2^m+1 是质数的假设不合，所以 m 没有奇约数，因此定理成立．

形状象 $2^{2^n}+1$ 的数，叫做**费马数**(P. D. Fermat，1601～1665)，用 F_n 表示，即

$$F_n=2^{2^n}+1,$$

当初费马猜测所有费马数都是质数．1732年欧拉(L，Euler，1707～1783)举出

$$2^{2^5}+1=641\times 6700417$$

否认了费马猜测．于是费马数也与梅审数一样，有的是质数，有的是合数，迄今已知的只有前五个费马数

$$F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65537$$

是质数，此外是否还有费马质数，也是数论中至今未得解决的难题．

高斯曾证明假如质数 p 是费马数，即 $p=F_n$，那末正 p 边形可以用圆规与直尺作出．

关于梅审数、费马数还有下面一个重要性质

假如 M_m，M_n 是两个不同的梅审数，由§1.2例3得

$$(M_m, M_n) = M_{(m,n)} = M_1 = 1.$$

于是我们有：

定理 4 任意两个梅审数互质．即当 $m \neq n$ 时，

$$(M_m, M_n) = 1.$$

与这类似，我们有：

定理 5 任意两个费马数互质．

证明 假定 $m = n + k$，那末

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{(2^{2^n})^{2^k} - 1}{2^{2^n} + 1}$$
$$= (2^{2^n})^{2^k - 1} - (2^{2^n})^{2^k - 2} + \cdots - 1,$$

即 $F_n \mid (F_m - 2)$．假如 d 是 F_m，F_n 的公约数，因为 $d \mid F_m$，$d \mid F_n$，所以 $d \mid 2$，但 F_n 是奇数，所以 $d \neq 2$，因此 $d = 1$，这就是说 F_m，F_n 只有公约数 1，所以 $(F_m, F_n) = 1$，于是定理成立．

习　题　1.4

1．试证不超过 F_n 的质数至少有 $n + 1$ 个，因此质数有无穷多个．

2．试证假如 $p > 2$，那末 M_p 没有质因数 3；假如 $p \neq 3$，那末 M_p 没有质因数 7．

§1.5　高斯函数$[x]$

假定 x 是实数，我们用记号$[x]$表示不大于 x 的最大整数，叫做高斯函数．譬如

$$[3]=3,\ [2.6]=2,\ \left[\frac{1}{3}\right]=0,$$

$$[-4.75]=-5,\ [x]=[[x]]$$

显然下面的式子成立．

$$x=[x]+a,\ 0\leqslant a<1,\ [x]\leqq x<[x]+1.$$

再§1.1定理1中 $q=\left[\frac{a}{|b|}\right]$，因此§1.1的(1)式，当 $b>0$ 时，可以写成 $a=\left[\frac{a}{b}\right]b+r$；当 $b<0$ 时，$a=-\left[\frac{a}{b}\right]b+r$.

例 1　$[x+y]\geqslant[x]+[y]$.

证　设

$$x=[x]+\alpha,\ y=[y]+\beta,\ 0\leqslant\alpha,\ \beta<1,$$

于是

$$x+y=[x]+[y]+\alpha+\beta,$$

但　$0\leqslant\alpha+\beta<2$，所以$[\alpha+\beta]=0$或1，因此

$$[x+y]=[x]+[y]\text{或}[x+y]>[x]+[y].$$

定理 1　假定 x 是任一实数，n 是正整数，那末

$$\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right].$$

证明　假定 $a=\left[\frac{x}{n}\right]$，那末

$$a\leqq\frac{x}{n}<a+1,$$

因此

$$na\leqq x<n(a+1),$$

但 na，$n(a+1)$ 都是整数，所以

$$na\leqq[x]<n(a+1),$$

于是

$$a \leqq \frac{[x]}{n} < a+1,$$

所以 $\left[\frac{[x]}{n}\right]=a$，因此定理成立.

定理 2 假定 x 是任意正实数，n 是正整数，那末

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]$$
$$=[nx],$$

上式叫做厄米特(C. Hermit，1822～1901)恒等式.

证明 设

$$f(x)=[nx]-[x]-\left[x+\frac{1}{n}\right]-\left[x+\frac{2}{n}\right]$$
$$-\cdots-\left[x+\frac{n-1}{n}\right]$$

那末 $f\left(x+\frac{1}{n}\right)$

$$=[nx+1]-\left[x+\frac{1}{n}\right]-\cdots-\left[x+\frac{n-1}{n}\right]-[x+1]$$
$$=[nx]-\left[x+\frac{1}{n}\right]-\cdots-\left[x+\frac{n-1}{n}\right]-[x]$$
$$=[nx]-[x]-\left[x+\frac{1}{n}\right]-\left[x+\frac{2}{n}\right]-\cdots-\left[x+\frac{n-1}{n}\right]$$
$$=f(x)$$

因为当 $0\leqslant x\leqslant\frac{1}{n}$时，$f(x)=0$，所以当 $0\leqslant x\leqslant\frac{2}{n}$时，$f(x)=0$，因此，当 x 是任意正实数时，$f(x)=0$，即厄米特恒等式成立．定理证毕.

下面是高斯函数的一个重要性质：

定理 3 假定 x 是正实数，n 是正整数，那末自 1 到 x 的整数中，n 的倍数有 $\left[\frac{x}{n}\right]$ 个.

证明 因为 $\left[\frac{x}{n}\right] \leqq \frac{x}{n} < \left[\frac{x}{n}\right] + 1$,

所以 $$\left[\frac{x}{n}\right] n \leqq x < \left\{\left[\frac{x}{n}\right] + 1\right\} n,$$

于是自 1 到 x 的整数中，n 的倍数只有

$$n,\ 2n,\ \cdots,\ \left[\frac{x}{n}\right] n,$$

它们总共 $\left[\frac{x}{n}\right]$ 个，因此定理成立.

例 2 求自 200 到 500 的整数中 7 的倍数的个数.

解 因为 $\left[\frac{500}{7}\right] = 71$, $\left[\frac{199}{7}\right] = 28$,

所以所求个数 $= 71 - 28 = 43$.

定理 4 在乘积 $n!$ 中，质数 p 的最高幂

$$p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^m}\right],$$

这里 $p^m \leqq n < p^{m+1}$.

证明 因为 p 是质数，如果 p 能够整除 $n!$，那末 p 必定能够整除 $1, 2, \cdots, n$ 中某数，但 $1, 2, \cdots, n$ 中 p 的倍数是下面 $\left[\frac{n}{p}\right]$ 个数

$$p,\ 2p,\ \cdots,\ \left[\frac{n}{p}\right] p,$$

于是 $n!$ 中 p 的最高幂就是

$$p \cdot 2p \cdot \cdots \left[\frac{n}{p}\right] p = \left[\frac{n}{p}\right]!\, p^{\left[\frac{n}{p}\right]}$$

中 p 的最高幂，因此

$$p(n!)=\left[\frac{n}{p}\right]+p\left(\left[\frac{n}{p}\right]!\right).$$

再同样，我们有

$$p\left(\left[\frac{n}{p}\right]!\right)=\left[\frac{\left[\frac{n}{p}\right]}{p}\right]+p\left(\left[\frac{\left[\frac{n}{p}\right]}{p}\right]!\right)$$

$$=\left[\frac{n}{p^2}\right]+p\left(\left[\frac{n}{p^2}\right]!\right),$$

所以 $$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+p\left(\left[\frac{n}{p^2}\right]!\right),$$

因为 $p^{m+1}>n$，这样继续进行，最后得 $\left[\frac{n}{p^{m+1}}\right]=0$，于是

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^m}\right],$$

因此定理成立．

特别，当 $n=p^r$ 时，

$$p(p^r!)=p^{r-1}+p^{r-2}+\cdots+1=\frac{p^r-1}{p-1}.$$

例 3 求 $50!$ 中 2 的最高幂．

解 $\left[\frac{50}{2}\right]=25$，$\left[\frac{50}{4}\right]=12$，$\left[\frac{50}{8}\right]=6$，

$\left[\frac{50}{16}\right]=3$，$\left[\frac{50}{32}\right]=1$，$\left[\frac{50}{64}\right]=0$，

所求最高幂

$$2(50!)=25+12+6+3+1=47,$$

即 $50!$ 只能够用 2^{47} 整除，解毕．

要注意的是定理 3 中 p 假如不是质数，定理不成立．譬如 $n=50$，$p=4$，由上面计算得 $4(50!)=12+3=15$．这结果与上例不一致，显然是错误的．

下面是上定理的一个重要应用.

定理 5 n 个相邻正整数的乘积能够用 $n!$ 整除,

证明 假定 $a>0$, 定理就是要求证明

$$\frac{(a+1)(a+2)\cdots(a+n)}{n!}=\frac{(a+n)!}{a!\,n!} \tag{1}$$

是整数. 由组合公式得知它是从 $a+n$ 个物体中每次取 n 个所得的组合数, 当然是整数. 假如不用这性质, 引用定理 3 也容易证明.

设 p 是任意质数, 由定理 3, 我们有

$$p((a+n)!)=\left[\frac{a+n}{p}\right]+\left[\frac{a+n}{p^2}\right]+\cdots,$$

$$p(a!)=\left[\frac{a}{p}\right]+\left[\frac{a}{p^2}\right]+\cdots,$$

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots,$$

因为 $$\left[\frac{a+n}{p^i}\right]\geqslant\left[\frac{a}{p^i}\right]+\left[\frac{n}{p^i}\right],$$

所以 $$\sum\left[\frac{a+n}{p^i}\right]\geqslant\sum\left[\frac{a}{p^i}\right]+\sum\left[\frac{n}{p^i}\right],$$

这就是说 $(a+n)!$ 中 p 的最高幂不小于 $a!\,n!$ 中 p 的最高幂, 因此(1)是整数. 定理证毕.

习 题 1·5

1. 证明 1000! 的末尾有 249 个 0.
2. 写出 30! 的标准分解式.
3. 求自 176 到 545 的整数中 13 的倍数的个数.
4. 求 2 在 $(2^r-1)!$ 中的最高幂.
5. 试求满足 $3(n!)=7$ 的 n.

6. 假如 x 是实数，a 是整数，那末 $[x+a]=[x]+a$.

7. 假如 a, b 是任意实数，那末

$[a]-[b]=[a-b]$ 或 $[a]-[b]=[a-b]+1$.

8. 求证

$$\frac{(n_1+n_2+\cdots+n_k)!}{n_1!\,n_2!\cdots n_k!}$$

是整数.

9. 假定 a, b 是互质的正数，求证

$$\left[\frac{a}{b}\right]+\left[\frac{2a}{b}\right]+\cdots+\left[\frac{(b-1)a}{b}\right]=\frac{(a-1)(b-1)}{2}.$$

10. 设 $r=\frac{4}{3}$，试证有无穷个正整数 n 使 $[nr]$ 为质数.

第二章 同余理论

上章讨论整除性是用约数来讨论的，而讨论的只是个别整数，怎样来全面地考虑整个的整数呢？我们用一个固定的数来除所有整数，根据余数我们可以把所有整数来分类，余数相同的同在一类，余数不相同的不同在一类，我们来讨论同一类的数有那些性质，不同类的数又有那些性质，这样我们就可以全面地来研究所有的整数了．以后各章我们都用这种同余理论来研究问题．这章，我们介绍同余理论的基本概念及一些基本性质．

同余概念是高斯在1800年前后创立的，在日常生活中也常常可以碰到．譬如本月2日是星期3，那末9，16，…都是星期3，这是因为它们用7除，余数都是2．古代我国所创的干支纪年也是这样的，它是以60作为除数的纪年法．

§2.1 同余概念与基本性质

假如两个整数 a，b 的差 $a-b$ 能够用正整数 m 整除，即 $m\mid(a-b)$，那末我们就叫 a 与 b 关于模 m **同余**，用符号

$$a\equiv b(\bmod m) \text{ 或 } a\equiv b(m)$$

表示，假如 $a-b$ 不能用 m 整除，即 $m\nmid(a-b)$，我们就说 a 与 b 关于模 m **不同余**，用符号

$$a\not\equiv b(\bmod m) \text{ 或 } a\not\equiv b(m)$$

表示.

譬如　$31\equiv 9 \pmod{11}$，$31\not\equiv 9 \pmod{10}$.

显然 a 与 b 关于 m 如果同余，那末以 m 除 a，b 得的余数相同，如果不同余，那末以 m 除 a，b 其余数不相同，反过来也成立. 假如 $a\equiv b \pmod m$，那末 $a=b+mt$，这里 t 是整数. 关于模 1，任意二整数 a，b 都同余，即 $a\equiv b \pmod 1$，关于模 2，偶数与偶数同余，奇数与奇数同余.

同余与普通的相等类似，也是等价关系，满足下面的等价律，即

定理 1　同余关系满足等价律：

1）自反律：任意整数 a 对于模 m 与自己同余，即

$$a\equiv a \pmod m.$$

2）对称律：假如 $a\equiv b \pmod m$，那末 $b\equiv a \pmod m$，

3）传递律：假如 $a\equiv b \pmod m$，$b\equiv c \pmod m$，那末

$$a\equiv c \pmod m.$$

这由定义可以立即推得.

二个同模的同余式能够与等式一样进行加，减，乘等运算.

定理 2　假如 $a_1\equiv b_1 \pmod m$，$a_2\equiv b_2 \pmod m$，那末

$$a_1\pm a_2\equiv b_1\pm b_2 \pmod m,\quad a_1a_2\equiv b_1b_2 \pmod m$$

$$ca_1\equiv cb_1 \pmod m,\ c \text{ 是任意整数.}$$

证明　因为　$m\mid(a_1-b_1)$，$m\mid(a_2-b_2)$；所以

$m\mid\{(a_1-b_1)\pm(a_2-b_2)\}$，即 $m\mid\{(a_1\pm a_2)-(b_1\pm b_2)\}$，因此 $a_1\pm a_2\equiv b_1\pm b_2 \pmod m$.

再由 $m\mid(a_1-b_1)$，我们有 $m\mid(ca_1-cb_1)$，因此

$$ca_1\equiv cb_1 \pmod m.$$

又，由 $a_1 \equiv b_1 \pmod m$，我们有 $a_1a_2 \equiv b_1a_2 \pmod m$，由 $a_2 \equiv b_2 \pmod m$，我们有 $b_1a_2 \equiv b_1b_2 \pmod m$，所以 $a_1a_2 \equiv b_1b_2 \pmod m$，于是定理成立．

特别，假如 $a \equiv b \pmod m$，那末对于任意整数 n，我们有

$$a^n \equiv b^n \pmod m.$$

等式两边可以用同一数来除，但同余式不一定能如此，譬如从 $15 \equiv 9 \pmod 6$ 不能推得 $5 \equiv 3 \pmod 6$，只有在某些情况下，才能这样．

定理 3 假如 $ca \equiv cb \pmod m$，并且 $(c, m) = 1$，那末

$$a \equiv b \pmod m.$$

证明 因为 $m \mid c(a-b)$，而 $(c, m) = 1$，所以 $m \mid (a-b)$，即 $a \equiv b \pmod m$．

一般我们有

定理 4 假如 $ca \equiv cb \pmod m$，$(c, m) = d$，那末

$$a \equiv b \left(\bmod \frac{m}{d}\right).$$

证明 由 $m \mid c(a-b)$．我们有 $\frac{m}{d} \Big| \frac{c}{d}(a-b)$，但这时 $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$，所以 $\frac{m}{d} \Big| (a-b)$，因此定理成立．

关于模不同的同余式，我们有：

定理 5 假定 $a \equiv b \pmod m$，又 $a \equiv b \pmod n$，如果 $k = [m, n]$，那末

$$a \equiv b \pmod k.$$

证明 因为 $m \mid (a-b)$，$n \mid (a-b)$，于是 $a-b$ 是 m, n 的公倍数，因此也是它们的最小公倍数的倍数，所以

$k|(a-b)$，即 $a\equiv b(\text{mod } k)$，定理成立．

上面这些性质虽然都很简单，但非常重要，读者不可等闲视之．

整数的某些整除性质用同余理论很容易得出，下面我们举例说明．

例 1 正整数 n 是 3 的倍数的必要充分条件是它的各个数字的和是 3 的倍数．

证 我们把 n 写成

$n=a_0+a_1 10+a_2 10^2+\cdots+a_{k-1}10^{k-1}$，$0\leqslant a_i<10$，

因为$10\equiv1(\text{mod } 3)$所以

$$\begin{aligned}&a_0+a_1 10+a_2 10^2+\cdots+a_{k-1}10^{k-1}\\&\equiv a_0+a_1+a_2+\cdots+a_{k-1}(\text{mod } 3),\end{aligned}$$

于是 $n\equiv0(\text{mod } 3)$的必要充分条件是

$$a_0+a_1+a_2+\cdots+a_{k-1}\equiv0(\text{mod } 3).$$

证毕．

同样，因为 $10\equiv1(\text{mod } 9)$，所以 n 是 9 的倍数的必要充分条件是

$$a_0+a_1+a_2+\cdots+a_{k-1}\equiv0(\text{mod } 9).$$

譬如 $n=637695$，它的各数字的和$6+3+7+6+9+5=36$是 9 的倍数，所以 n 是 9 的倍数，当然也是 3 的倍数．

例 2 2 位以上的数能够用 4 整除的必要充分条件是它最后两个数字组成的数能够用 4 整除．

譬如$7316=73\cdot100+16$，因为 $100\equiv0(\text{mod } 4)$，$16\equiv0(\text{mod } 4)$，所以 $7316\equiv0(\text{mod } 4)$．

例 3 求正整数 n 能够用 7 整除的必要充分条件．

解 因为 $1000\equiv-1(\text{mod } 7)$，我们把 n 写成

$$n=a_0+a_1 1000+a_2 1000^2+\cdots+a_{k-1}1000^{k-1},$$
$$0\leq a_i<1000,$$
即得所求的必要充分条件
$$(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$$
$$=\sum_{i=0}^{k-1}(-1)^i a_i\equiv 0\pmod 7.$$

譬如 $n=637693=693+637\cdot 1000$，这时 $a_0=693$，$a_1=637$，因为
$$a_0-a_1=693-637=56\equiv 0\pmod 7.$$
所以 637693 是 7 的倍数.

例 4　试证 $x^2+y^2=z^2$ 没有都是质数的解.

证　用反证法，假如 $x=a$，$y=b$，$z=c$ 是质数解，如果 $a=2$，由 $c^2-b^2=a^2$ 得 $(c+b)(c-b)=4$，因此 $c+b=4$，$c-b=1$，所以 $c=\frac{5}{2}$，此不可. 于是 a，b 都是奇数，因此 $a^2\equiv 1\pmod 4$，$b^2\equiv 1\pmod 4$，所以 $a^2+b^2\equiv 2\equiv c^2\pmod 4$，于是 $2\mid c$，这显然不可，这就是说 a，b，c 不能都是质数，例得证.

习　题　2.1

1. 假如 $a\equiv b\pmod m$，那末 $(a,\ m)=(b,\ m)$.

2. 试证一个整数是 11 的倍数的必要充分条件是这个数的奇位数字的和与偶位数字的和的差是 11 的倍数.

3. 3 位以上的数能够用 8 整除的必要充分条件是它最后三个数字组成的数能够用 8 整除.

4. 试求正整数 n 能够用 13 整除的必要充分条件，因而

判别 13 是否是 637693 的因数？

5. 假定 $a=28997$，$b=39495$，有人计算它们的积 $c=1145236415$，这个结果是否正确？

6. 假定 a,b 是任意整数，p 是质数，试证

$$(a+b)^p\equiv a^p+b^p \pmod p.$$

§2.2 完全剩余系、简化剩余系

假定 m 是正整数，因为任一整数用 m 去除得到的最小非负剩余必定是 0，1，…，$m-1$ 中一数，也就是说任一整数对于模 m 必定与 0，1，…，$m-1$ 中某一数同余. 因此我们把所有与 0 同余的数作为一类，所有与 1 同余的数作为一类等等，以及所有与 $m-1$ 同余的数作为一类，这样的类叫做关于模 m **的同余类**，显然任一数必定属于一类而且只属于一类. 再我们容易得知同一类中任意二数都同余，不同类中任意二数都不同余，a 所在的同余类中数是所有形状象

$$a+mt,\ t \text{ 是任意整数},$$

的数.

对于模 m，我们可以把所有整数分成 m 类，从每类中任取一数就得到 m 个数，这 m 个数叫做 m **的完全剩余系**. m 的完全剩余系，通常采用的是由 m 个非负的最小整数 0，1，2，…，$m-1$ 组成的，有时为了计算方便，我们也常取绝对值是最小的 m 个数，即当 m 是奇数时，取

$$-\frac{m-1}{2},\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ \frac{m-1}{2},$$

当 m 是偶数时，取

$$-\frac{m}{2}+1,\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ \frac{m}{2}$$

或 $$-\frac{m}{2},\quad \cdots,\ -1,\ 0,\ 1,\ \cdots,\ \frac{m}{2}-1,$$

下面是 k 个数形成 m 的完全剩余系的必要充分条件.

定理 1 k 个数 a_1, a_2, $\cdots$, a_k 形成 m 的完全剩余系的必要充分条件是

1. $k=m$, 2. $a_i\not\equiv a_j \pmod m$, $i\neq j$.

证明 假如 a_1, a_2, $\cdots$, a_k 是 m 的完全剩余系，根据定义，a_1, $a_2,\cdots$, a_k 是从 m 个不同的同余类中各取一数而成，因此 a_i 的个数是 m 即 $k=m$, 又因为任意二数 a_i, $a_j(i\neq j)$ 不同在一同余类，所以 $a_i\not\equiv a_j \pmod m$, 于是必要条件成立.

反过来，假如 a_1, a_2, $\cdots$, a_m 中任意 $a_i\not\equiv a_j \pmod m$, $i\neq j$, 那末 a_i, a_j 不在同一同余类，因此这 m 个数 a_1, a_2, $\cdots$, a_m 是分布在 m 个互异的同余类中，每类一数，所以 a_1, a_2, $\cdots$, a_m 是 m 的完全剩余系，充分条件成立，因此定理得证.

于是任意 m 个互不同余的数构成 m 的完全剩余系.

定理 2 假定 a_1, a_2, $\cdots$, a_m 是 m 的完全剩余系，$(a,\ m)=1$, 那末

$$aa_1+b,\ aa_2+b,\ \cdots,\ aa_m+b,\quad b\text{是任意数},$$

也是 m 的完全剩余系.

证明 由定理1，只要证明 $aa_i+b\not\equiv aa_j+b \pmod m$, $i\neq j$, 定理就告成立，下面我们用反证法来证明，假如

$$aa_i+b\equiv aa_j+b \pmod m,\quad i\neq j,$$

那末 $aa_i\equiv aa_j \pmod m$, 但 $(a,\ m)=1$, 由§2.1定理3我们即得 $a_i\equiv a_j \pmod m$, 这与 a_1, $\cdots$, a_m 是 m 的完全剩余系的

假设不合，因此定理成立.

在 m 的一个完全剩余系中有的数与 m 互质，有的数与 m 不互质，所有与 m 互质的数构成的系，叫做 m 的**简化剩余系**. 因为 1 与任何数互质. 所以任意正整数都有简化剩余系. 再因为当 a 与 m 互质时，a 所在的同余类中的数都与 m 互质，当 a 与 m 不互质时，a 所在的同余类中的数都与 m 不互质，所以简化剩余系中数的个数与原来所取的完全剩余系无关，由 m 唯一决定，欧拉(L. Euler 1707—1783)用 $\varphi(m)$ 来表示，叫做**欧拉函数**. 也就是说 $\varphi(m)$ 是表示所有不大于 m 且与 m 互质的正整数的个数.

譬如不大于 5 且与 5 互质的正数只有 1，2，3，4. 因此 $\varphi(5)=4$. 又如 1，3，7，9 是所有不大于 10 且与 10 互质的正数，因此 $\varphi(10)=4$.

显然 $\varphi(1)=1$，一般正整数 n 假如是质数，那末 $\varphi(n)=n-1$，假如是合数，那末 $\varphi(n)<n-1$. 于是对于任意数 n，我们有 $\varphi(n)\leqq n-1$. 再 $\varphi(n)=n-1$ 的必要充分条件是 n 是质数.

同完全剩余系一样，我们有：

定理 3 k 个整数 a_1，a_2，…，a_k 是 m 的简化剩余系的必要充分条件是：

1. $k=\varphi(m)$； 2. $a_i\not\equiv a_j \pmod m$，$i\neq j$；

3. $(a_i, m)=1$.

证明 因为 $a_i\not\equiv a_j \pmod m$，所以 a_1，a_2，…a_k 中每一数各在一同余类，再由 $k=\varphi(m)$，$(a_i, m)=1$，所以 a_1，a_2，…，a_k 是 m 的完全剩余系中所有与 m 互质的数，因此它是 m 的简化剩余系，充分条件成立. 必要条件是显然的，因此

定理成立.

于是任意 $\varphi(m)$ 个与 m 互质且又对于 m 不同余的数构成 m 的简化剩余系.

定理 4 假定 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是 m 的简化剩余系，$(a, m)=1$，那末 $aa_1, aa_2, \cdots, aa_{\varphi(m)}$ 也是 m 的简化剩余系.

证明 因为 $a_i \not\equiv a_j \pmod m$，$(a, m)=1$，所以 $aa_i \not\equiv aa_j \pmod m$，再因为 $(a_i, m)=1$，$(a, m)=1$，所以 $(aa_i, m)=(a_i, m)=1$，于是由定理 3，$aa_1, \cdots, aa_{\varphi(m)}$ 是 m 的简化剩余系，因此定理成立.

引用简化剩余系的性质，我们不难证明下面的**欧拉定理**. 它是 1760 年欧拉首先证明的，是数论中一个重要定理，有广泛的应用.

定理 5 假定 $(a, m)=1$，那末

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

证明 假定 $x_1, x_2, \cdots x_{\varphi(m)}$ 是 m 的简化剩余系，由定理 4，得知 $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 也是 m 的简化剩余系，于是 $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 中任一数必与 $x_1, x_2, \cdots, x_{\varphi(m)}$ 中某数关于 m 同余，即

$$a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)} \equiv x_{i1} x_{i2} \cdots x_{i\varphi(m)}$$

$$= x_1 x_2 \cdots x_{\varphi(m)} \pmod m,$$

但 $(x_i, m)=1$，所以 $(x_1 x_2 \cdots x_{\varphi(m)}, m)=1$，因此由 §2.1 定理 3，我们可以把 $x_1 x_2 \cdots x_{\varphi(m)}$ 消去，于是定理成立.

特别，当 m 是质数 p，即 $m=p$ 时，$\varphi(p)=p-1$，于是我们有下面费马定理，它是 1640 年费马提出，1736 年欧拉证明的.

定理 6 假定$(a, p)=1$，p是质数，那末

$$a^{p-1}\equiv 1 \pmod p.$$

因为后面有费马大定理，所以有人把这定理又叫做费马小定理。

我们用a乘上式，即得$a^p\equiv a \pmod p$，显然当$p\mid a$时这式也是成立的，因此不论a是何数，只要p是质数，我们有

$$a^p\equiv a \pmod p.$$

要注意的是上面费马定理的逆不成立，这就说当$a^{m-1}\equiv 1 \pmod m$时，m不一定是质数，譬如$2^{340}\equiv 1 \pmod{341}$，这时$341=11\times 31$不是质数，但在某些特殊情况下，费马定理的逆还是能成立。

我们先证下面性质以备引用。

例 1 假如d是满足$a^x\equiv 1 \pmod m$的所有正整数x中的最小数，那末$d\mid x$，

证 命$x=qd+r$，$0\leqq r<d$，因为

$$a^x=a^{qd+r}=a^{qd}\cdot a^r=(a^d)^q a^r,$$

所以$a^r\equiv 1 \pmod m$，于是$r=0$，因此$x=qd$，例成立。

定理 7 假如$a^{m-1}\equiv 1 \pmod m$，并且对于$m-1$的任一真约数n，$a^n\not\equiv 1 \pmod m$，那末m是质数。

证明 根据上例，$m-1$是满足$a^x\equiv 1 \pmod m$的最小数，由欧拉定理，$a^{\varphi(m)}\equiv 1 \pmod m$，于是$\varphi(m)\geqq m-1$。但不论$m$是何数，只要$m>1$就有$\varphi(m)\leqq m-1$，因此$\varphi(m)=m-1$，这就是说$m$是质数，所以定理成立。

譬如，47是质数，可以根据上定理证明如下：

因为$47-1=46$的因子只有1，2，23，46，而

$$45^{23}=(47-2)^{23}\equiv(-2)^{23}\equiv-1\pmod{47},$$

显然 $45\not\equiv1\pmod{47}$，$45^2\not\equiv1\pmod{47}$．所以 47 是质数．

再要注意的是上定理的逆也不成立，即当 m 是质数时，可能有 $n\mid(m-1)$ 使 $a^n\equiv1\pmod m$，譬如 $m=5$，$a=4$，这时 $4^2\equiv1\pmod 5$．

例 2 假定 p 是质数，q 是 2^p-1 的质因数，试证 $q>p$．

证 当 $p=2$ 时例显然成立，因此，假定 p 是奇数．因为 $q\mid(2^p-1)$，所以 $2^p\equiv1\pmod q$．再由费马定理得 $2^{q-1}\equiv1\pmod q$，如果 $p=q$，那末 $2^{p-1}\equiv2^p$，这显然是矛盾．如果 $q<p$，由 $(p,\ q-1)=1$ 得

$$ap+b(q-1)=1,$$

因此 $$2=2^{ap+b(q-1)}\equiv1\pmod q$$

这又是矛盾．所以 $q>p$．证毕．

于是如果 q 是梅审数 M_p 的质因数，那末 $q>p$．

下面是关于梅审数与费马数的质因数的性质，是费马定理的一个应用．

定理 8 梅审数 $M_p(p>2)$ 的质因数是 $2pt+1$ 形状．

证明 假定 q 是 $M_p=2^p-1$ 的质因数，那末 $2^p\equiv1\pmod q$，因为 p 是质数，所以它是适合上关系的最小数，但由费马定理，$2^{q-1}\equiv1\pmod q$，所以 $p\mid(q-1)$，又因为 q 是奇数，所以 $2\mid(q-1)$，于是 $2p\mid(q-1)$ 即 $q=2pt+1$，因此定理成立．

譬如 $M_{11}=2^{11}-1=2047$，这时不大于 $\sqrt{2047}=45\cdot2$ 而形状是 $2\cdot11t+1=22t+1$ 的质数只有 $22\cdot1+1=23$，以 23 除之得 $2047=23\times89$，所以 M_{11} 是合数．

定理 9 $a^{2^n}+1\,(a>1)$ 的奇质因数是 $2^{n+1}t+1$ 形状，

证明　用数学归纳法证明

当 $n=0$ 时，定理显然成立，假定 $n-1$ 时定理成立，即

$$a^{2^{n-1}}+1\equiv 0\,(q_1),\quad q_1=2^n t_1+1,$$

设 $a^{2^n}+1\equiv 0\,(q)$．即 $(a^2)^{2^{n-1}}+1\equiv 0\,(q)$，由归纳法假设得 $q=2^n t+1$．因为

$$(a^{2^n})^t\equiv(-1)^t\,(q),\quad 即\quad a^{q-1}\equiv(-1)^t\,(q)$$

由费马定理得 $(-1)^t\equiv 1\,(q)$，因为 $q>2$，所以 t 是偶数，即 $t=2t_2$，于是 $q=2^{n+1}t_2+1$，证毕．

定理 10　费马数 $F_n\,(n\geqslant 2)$ 的质因数是 $2^{n+2}t+1$ 形状．

证明①　假定 q 是 F_n 的质因数，如果我们能够证明 $F_{n-1}^{2^{n+1}}+1\equiv 0\,(F_n)$，那末 q 也是 $F_{n-1}^{2^{n+1}}+1$ 的质因数，因此根据定理 9 得 $q=2^{n+2}t+1$，定理即告成立．因为

$$\begin{aligned}F_{n-1}^{2^{n-1}}&=(2^{2^{n-1}}+1)^{2^{n+1}}=(2^{2^n}+2^{2^{n-1}+1}+1)^{2^n}\\&\equiv(2^{2^{n-1}+1})^{2^n}\equiv(2^{2^n})^{2^{n-1}+1}\equiv(-1)^{2^{n-1}+1}\\&\equiv -1\,(F_n)\end{aligned}$$

所以
$$F_{n-1}^{2^{n+1}}+1\equiv 0\,(F_n).$$

于是定理成立．

譬如，$F_5=2^{2^5}+1$，不大于 $2^{2^4}=65536$ 而形状是 $2^{5+2}t+1=128t+1$ 的质数只有 257，641，以它们除 F_5 验证，得知 641 是 F_5 的因数，即 $F_5=641\cdot 6700417$，因此 F_5 是合数．

习　题　2.2

1．假设 p 是质数，并且 $(a,\ p)=1$，那末

1）当 a 是奇数时，$a^{p-1}+(p-1)^a\equiv 0\,(\mathrm{mod}\ p)$

① 这证明是邹亚清给出的．

2）当 a 是偶数时，$a^{p-1}-(p-1)^a\equiv 0 \pmod p$

2. 试证两个相邻偶数的乘积是 8 的倍数，因此引用费马定理，证明当 p 是大于 5 的质数时，$p^4\equiv 1 \pmod{240}$.

3. 试证大于 3 的任意二个质数的平方的差是 24 的倍数.

4. 假设 p 是不等于 3 又不等于 7 的任意奇质数，那末

$$p^6\equiv 1 \pmod{168}.$$

5. 假设奇质数 p，q 满足 $2p=q+1$，并且 x 与 2，p，q 都互质. 试证 $x^{2(p-1)}\equiv 1 \pmod{16pq}$.

6. 假如 p，q 是任意二个不同的质数，试证

$$p^{q-1}+q^{p-1}\equiv 1 \pmod{pq}$$

§2.3 欧 拉 函 数

我们知道欧拉函数 $\varphi(m)$ 是表示 m 的简化剩余系中所含数的个数，也是小于 m 并且与 m 互质的正整数的个数，它是由 m 唯一决定的. 这节我们来给出计算 $\varphi(m)$ 的一般公式.

我们先由简单的情况开始，我们知道，当 p 是质数时，$\varphi(p)=p-1$，在 p^k 的完全剩余系中与 p^k 不互质的数只有 p 的倍数

$$p,\ 2p,\ \cdots,\ p^{k-1}p,$$

这共有 p^{k-1} 个，其余

$$p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$$

个数都与 p^k 互质，因此 p^k 的简化的剩余系含有

$p^k\left(1-\dfrac{1}{p}\right)$ 个数，即

$$\varphi(p^k) = p^k\left(1-\frac{1}{p}\right) \tag{1}$$

对于二个互质数的乘积，我们有：

定理 1 假定$(a, b)=1$，那末

$$\varphi(ab)=\varphi(a)\varphi(b).$$

证明 假定$x_1, \cdots, x_{\varphi(a)}$; $y_1, \cdots, y_{\varphi(b)}$分别是$a$, b的简化剩余系，显然

$$bx_i+ay_j, \qquad i=1,\cdots,\varphi(a), j=1,\cdots,\varphi(b), \tag{2}$$

中含有$\varphi(a)\varphi(b)$个数，下面我们用反证法来证明(2)就是ab的简化剩余系，因此定理就告成立。

假如 $\quad bx_i+ay_j\equiv bx_k+ay_l \pmod{ab}$,

那末 $\quad bx_i+ay_j\equiv bx_k+ay_l \pmod{a}$.

于是 $\quad bx_i\equiv bx_k \pmod{a}$,

即 $\quad x_i\equiv x_k \pmod{a}$.

但x_i, x_k是a的简化剩余系中数，所以$x_i=x_k$，因此$i=k$，同样，我们有$y_j=y_l$，因此$j=l$，这就是说(2)中任意二数对模ab都不同余。

再因为$(x_i, a)=1$，$(b, a)=1$，所以$(bx_i, a)=1$，因此$(bx_i+ay_j, a)=1$，同样$(bx_i+ay_j, b)=1$，于是$(bx_i+ay_j, ab)=1$，所以(2)中任一数都与ab互质，假如我们又能够证明任意与ab互质的数z必与(2)中某个bx_i+ay_j关于ab同余，那末(2)就是ab的简化剩余系了。

假定$(z, ab)=1$，因为$(a, b)=1$，所以$bx_0+ay_0=1$，于是存在整数x, y使$z=bx+ay$，但$(z, a)=1$，即$(bx+ay, a)=1$，所以$(bx, a)=1$，因此$(x, a)=1$，于是$x\equiv x_i \pmod{a}$。同样，我们有$y\equiv y_j \pmod{b}$，因此$bx\equiv bx_i$,

$ay \equiv ay_j \pmod{ab}$， 所以 $bx+ay \equiv bx_i+ay_j \pmod{ab}$； 即 $z \equiv bx_i+ay_j \pmod{ab}$，这就是说与 ab 互质的数必与(2)中某一数同余，于是(2)是 ab 的简化剩余系，所以定理成立.

有了上面这些结果，一般 $\varphi(m)$ 的公式我们就容易推得.

假如 $m=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$，由定理1，容易得知

$$\varphi(m)=\varphi(p_1^{m_1})\varphi(p_2^{m_2})\cdots\varphi(p_k^{m_k}),$$

再由(1)即得主要公式

定理 2 假定 $m=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$，那末

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

或

$$\varphi(m)=p_1^{m_1-1}p_2^{m_2-1}\cdots p_k^{m_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).$$

譬如 $\varphi(300)=\varphi(2^2\cdot3\cdot5^2)$

$$=2^2\cdot3\cdot5^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=80.$$

显然 当 $m>2$ 时，$\varphi(m)$ 是偶数，当 $n\mid m$ 时，

$$\varphi(n)\mid\varphi(m).$$

例 求满足下式的所有正整数 m，n

$$\varphi(mn)=\varphi(m)+\varphi(n),$$

解 由定理2，我们容易得到

$$\varphi(mn)=\frac{d\varphi(m)\varphi(n)}{\varphi(d)},\quad d=(m,\ n)$$

因此，给出的式可以写成

$$\frac{1}{a}+\frac{1}{b}=d,\quad a=\frac{\varphi(m)}{\varphi(d)},\quad b=\frac{\varphi(n)}{\varphi(d)}$$

因为 a，b 都是正整数，所以 $d=2$，即 $a=b=1$ 或 $d=1$，即 $a=b=2$. 在前者 $\varphi(m)=\varphi(n)=1$，此时 $m=n=2$，在后者

$\varphi(m)=\varphi(n)=2$，此时 m，n 中有一为3，他一为4．这就是所求数，解毕．

最后我们来介绍 $\varphi(m)$ 的二个基本性质．

定理 3 假定 d 是正整数 m 的正约数，那末 m 的完全剩余系中与 m 的最大公约数是 d 的数的个数是 $\varphi(\frac{m}{d})$．

证明 在 m 的完全剩余系 1，2，…，m 中，d 的倍数是形状象 kd，$1\leqq k\leqq\frac{m}{d}$，的数，假如 $(kd, m)=d$，那末 $(k,\frac{m}{d})=1$，这就是说只有 k 是 $1,2,\cdots,\frac{m}{d}$ 中与 $\frac{m}{d}$ 互质的数时，kd 与 m 的最大公约数才是 d，所以 k 的个数等于 $\varphi(\frac{m}{d})$，于是定理成立．

定理 4 假定 d_1，d_2，$\cdots d_{T(m)}$ 是正整数 m 的所有正约数，那末

$$\sum_{i=1}^{T(m)}\varphi(d_i)=m.$$

证明 因为 d_1，…，$d_{T(m)}$ 是 m 的所有正约数，所以 $\frac{m}{d_1}$，…，$\frac{m}{d_{T(m)}}$ 也是 m 的所有正约数，于是

$$\sum_{i=1}^{T(m)}\varphi(d_i)=\sum_{i=1}^{T(m)}\varphi\left(\frac{m}{d_i}\right).$$

再因为在 m 的完全剩余系 1，2，…，m 中任一数与 m 的最大公约必定是 d_1，…，$d_{T(m)}$ 中某一数，把 1，2，…，m 中所有与 m 最大公约数相同的数作为一类，那末 1，2，…，m 中数可以分为 $T(m)$ 个类，各类中所含数的个数分别

为

$$\varphi\left(\frac{m}{d_1}\right),\ \cdots,\ \varphi\left(\frac{m}{d_{T(m)}}\right),$$

于是$\sum_{i=1}^{T(m)}\varphi\left(\frac{m}{d_i}\right)=m$, 即$\sum_{i=1}^{T(m)}\varphi(d_i)=m$, 因此定理成立.

譬如 $m=30$ 时, $d_i=1$, 2, 3, 5, 6, 10, 15, 30, 这时

$$\begin{aligned}&\varphi(1)+\varphi(2)+\varphi(3)+\varphi(5)+\varphi(6)\\&\quad+\varphi(10)+\varphi(15)+\varphi(30)\\&\quad=1+1+2+4+2+4+8+8=30.\end{aligned}$$

习 题 2.3

1. 求 $13^{1956}\equiv?\pmod{60}$.

2. 假如 $\varphi(m)=$ 奇数, 问 $m=?$

3. 试证使 $\varphi(m)=14$ 的数 m 不存在.

4. 假如 $n=2n_1$, $(2, n_1)=1$, 那末 $\varphi(n)=\varphi(n_1)$, 因而证明

$$\varphi(x)=4n-2,\ n>1$$

的一切解 x 或为 p^a 或为 $2p^a$ 的形状, 其中 p 是形状是 $4k-1$ 的质数.

5. 假设 $(m_1, m_2)=1$, x_1, $\cdots$, x_k 是 m_1 的完全剩余系, y_1, $\cdots$, y_l 是 m_2 的完全剩余系, 试证 $m_2x_i+m_1y_j$, $i=1$, $\cdots$, k; $j=1$, $\cdots$, l 是 $m=m_1m_2$ 的完全剩余系.

6. 证明分母是正整数 n 的既约真分数的个数等于 $\varphi(n)$.

7. 证明分母不大于 n 的既约真分数的个数等于

$$\varphi(2)+\cdots+\varphi(n).$$

8. 假如 p 是质数，试证

$$\varphi(1)+\varphi(p)+\cdots+\varphi(p^k)=p^k.$$

9. 假如 $(a, b)=d$，证明

$$\varphi(ab)=\frac{d\varphi(a)\varphi(b)}{\varphi(d)}.$$

10. 试证所有小于 $n(>1)$ 并且与 n 互质的正整数的和为 $\frac{n}{2}\varphi(n)$.

11. 求所有满足 $\varphi(m)=\frac{m}{p}$ 的正整数 m 及质数 p.

12. 求所有满足 $x^{\varphi(y)}=y$ 的正整数 x，y.

第三章　不定方程

方程的个数少于未知量的个数而且未知量又须受某种限制(如整数或正整数等)，这样一类的方程叫做**不定方程**，三世纪初希腊数学家刁番图(Diophantus，约246～330)曾大力研究过这类方程，因此不定方程也叫做刁番图方程．这章我们主要是讨论求解最简单的不定方程．

§3.1　一次不定方程

下面是主要定理：

定理　一次不定方程

$$ax+by=c\qquad a,\ b,\ c\text{都是整数}\qquad(1)$$

有整数解的必要充分条件是 $d\mid c$，这里 $d=(a,\ b)$．假如 $x=x_0$，$y=y_0$ 是(1)的一个解，那末它的任一解可以写成

$$x=x_0+\frac{b}{d}t,\quad y=y_0-\frac{a}{d}t,$$

这里 t 是任意整数．

证明　定理中的必要条件是显然的，下面只证明充分性．假如 $d\mid c$，用 d 除(1)式得

$$a'x+b'y=c'.\qquad(2)$$

这时 $(a',\ b')=1$．根据§1,2定理6或者直接引用欧几里得算法，我们有整数 x_0'，y_0' 满足

$$a'x_0' + b'y_0' = 1.$$

于是
$$a'c'x_0' + b'c'y_0' = c'$$

因此 $x = c'x_0'$，$y = c'y_0'$ 是(2)的解，当然也是(1)的解。

假定 $x = x_0$，$y = y_0$ 是(1)的解，那末

$$a'x_0 + b'y_0 = c'$$

与(2)相减得

$$a'(x_0 - x) = b'(y - y_0),$$

因为$(a', b') = 1$，所以 $a' \mid (y - y_0)$，命

$$y - y_0 = -a't$$

得

$$x - x_0 = b't$$

因此
$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

是(1)的解． 于是定理得证．

例 1 解不定方程

$$525x + 231y = 42$$

解 因为$(525, 231) = 21$，用 21 除上式得

$$25x + 11y = 2.$$

又因为$(25, 11) = 1$，由 §1.2 的欧几里得算法，得

$$25(4) + 11(-)9 = 1,$$

因此 $x = 2 \cdot 4 = 8$，$y = 2(-9) = -18$ 是所给方程的一组解，于是所求的一般解

$$x = 8 + 11t, \qquad y = -18 - 25t.$$

显然它没有正整数解．解毕．

当(1)的系数不大时，有时我们可以用视察法求得其解．此外，我们还可以用下面逐渐减小系数的方法，这方法有时

还比较简便．

例 2　求不定方程

$$7x+19y=213$$

的正整数解．

解　用最小的系数 7 除上式得

$$x=\frac{213-19y}{7}=30-2y+\frac{3-5y}{7}$$

因为 x 是整数，y 也是整数，所以

$$\frac{3-5y}{7}=u$$

也是整数．即

$$5y+7u=3.$$

又用 5 除上式两边，得

$$y=\frac{3-7u}{5}=-u+\frac{3-2u}{5},$$

因此我们有

$$2u+5v=3$$

显然 $u=-1$，$v=1$ 是它的一个解，所以 $x=25$，$y=2$．于是所求的一般解为

$$x=25+19t,\quad y=2-7t.$$

假如要求解是正整数，那末 $25+19t>0$，$2-7t>0$，即

$$-\frac{25}{19}<t<\frac{2}{7}$$

因此 $t=0$，$t=-1$．于是所求正整数解为

$$x=25,\ y=2;\quad x=6,\ y=9.$$

三元或多元一次不定方程也可以类似地求解．

例 3　解　$50x+45y+38z=10$

解 我们把它分为两个二元一次方程来求解

$$50x+45y=5t,\quad 5t+36z=10.$$

因为 $50(t)+45(-t)=5t$，$5(-70)+36(10)=10$，所以上面两个方程的解分别为

$$\begin{cases}x=t+9k_1\\y=-t-10k_1\end{cases}\qquad\begin{cases}t=-70+36k_2\\z=10-5k_2\end{cases}$$

消去 t 就得到所求解

$$\begin{cases}x=-70+9k_1+36k_2\\y=70-10k_1-36k_2\\z=10-5k_2\end{cases}$$

或

$$\begin{cases}x=2+9k_1+36k_2\\y=-2-10k_1-36k_2\\z=-5k_2\end{cases}$$

这里 k_1，k_2 是任意整数.

我们也可以同例 2 一样用逐渐减小系数的方法求解.

因为 36 是系数中最小的，我们可以把所给方程写成

$$36(x+y+z)+14x+9y=10,$$

设 $x+y+z=k_1$，得

$$14x+9y+36k_1=10,$$

又
$$9(x+y+4k_1)+5x=10,$$

设 $x+y+4k_1=5k_2$，得

$$5x+45k_2=10,$$

即
$$x+9k_2=2.$$

于是得所求解

$$\begin{cases} x = 2 - 9k_2 \\ y = -2 - 4k_1 + 14k_2 \\ z = 5k_1 - 5k_2 \end{cases}$$

这里 k_1，k_2 是任意整数．前后两组解显然是一致的．解毕．

例 4　试证不定方程

$$a_1x_1 + \cdots + a_nx_n = c, \quad a_i, \ c \text{ 都是整数，}$$

有整数解的必要充分条件是

$$d = (a_1, \ \cdots, \ a_n) \mid c.$$

证　必要条件是显然的．下面只证明充分条件．

由 § 1.2，我们有 $b_1 \cdots$，b_n 使

$$a_1b_1 + \cdots + a_nb_n = d.$$

设 $c = dc_1$，于是

$$a_1(b_1c_1) + \cdots + a_n(b_nc_1) = dc_1 = c,$$

即 $x_1 = b_1c_1$，$\cdots$，$x_n = b_nc_1$ 是方程的解，证毕．

例 5　试证 $x^{-1} + y^{-1} = z^{-1}$，$(x, \ y, \ z) = 1$，的正整数解是且仅是

$$x = a(a+b), \ y = b(a+b), \ z = ab$$

这里 a，$b > 0$，$(a, \ b) = 1$．

证　充分性是显然的，下面证明必要性．

设 x，y，z 是方程的解，$(x, \ y) = c$，即 $x = ca$，$y = cb$，$(a, \ b) = 1$．于是

$$z^{-1} = x^{-1} + y^{-1} = \frac{a+b}{cab},$$

即
$$z = \frac{cab}{a+b}.$$

因为 $(a, \ b) = 1$，所以 $(ab, \ a+b) = 1$，因此 $(a+b) \mid c$，设 $c = c'(a+b)$．于是 $z = c'ab$．因为 $(x, \ y, \ z) = 1$，所以

$$(ca,\ cb,\ c'ab)=(c(a,\ b),\ c'ab)$$
$$=(c'(a+b),\ c'ab)=c'=1$$

因此例成立.

例 6　求 $x^{-1}+y^{-1}=n^{-1}$ 的整数解的个数，其中 x，y 都是正整数且不相等.

解　设 $x=n+r$，$y=n+s$，由给出方程即得 $n^2=rs$. 因此所求正整数解的个数为 $T(n^2)-1$.

习　题　3.1

1. 解下列不定方程

   1）$525x+231y=42$,

   2）$8x-18y+10z=16$,

   3）$4x+10y+14z+6t=20$.

2. 求下列不定方程的正整数解

   1）$19x+20y=1909$,

   2）$x^2+xy-6=0$,

   3）$y-\dfrac{x+3y}{x+2}=1$.

3. 解线性方程组

$$\begin{cases}x+2y+3z=10\\ x-2y+5z=4\end{cases}$$

4. 求所有用 4 除余 1 的两位数的和.

5. 有 A，B 两种物品，13 个 A 的价与 5 个 B 的价的和是 141 元，假如 A，B 的价都是整数，问 A，B 的价各若干?

6. 鸡翁一值钱五，鸡母一值钱三，鸡雏三值钱一，百钱买百鸡，问鸡翁、鸡母、鸡雏各若干?（这题系张丘建《算

经》卷下的最后一题，该书在隋代还广泛流传，但作者生、卒年仍不易考）.

7. 方程 $axy+bx+cy+d=0$ 能否有无穷多组整数解，其中 $0\neq a$, b, c, d 都是整数.

§3.2 商高不定方程

下面我们讨论叫做商高（生于公元前580～568之间，卒于公元前501～500之间）或毕达哥拉斯（Pythagoras，572～492 B.C.）方程的二次不定方程

$$x^2+y^2=z^2 \qquad (1)$$

的整数解.

假如 x, y, z 中有一为零，譬如 $x=0$，那末 $y=\pm z$. 因此我们可以假定 x, y, z 都大于零，再我们还可以假定 $(x, y, z)=1$，因此 $(x, y)=1$，这时 x, y 必定是一为偶数，一为奇数，这是因为如果 x, y 都是奇数，那末 $x^2=4n+1$, $y^2=4m+1$，于是 $x^2+y^2=4(m+n)+2$，但 $z^2=4k$ 或 $4k+1$，显然这时 $x^2+y^2\neq z^2$. 因此我们假定 y 是偶数.

定理 1 不定方程（1）适合条件

$x>0$, $y>0$, $z>0$, $(x, y)=1$, y 是偶数的一切正整数解可以表为

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2. \qquad (2)$$

这里 $a>b>0$, $(a, b)=1$，并且 a, b 一为奇数，一为偶数.

证明 我们容易验证（2）的确是适合给出条件的解.

假如 x, y, z 是（1）适合定理中给出条件的解，因为 $(x, y)=1$，所以 $(y, z)=1$. 于是 $(z+y, z-y)=1$ 或 2.

但 y 是偶数，z 是奇数，所以 $(z+y,\ z-y)\neq 2$，因此 $(z+y,\ z-y)=1$. 于是由

$$x^2=(z+y)(z-y)$$

我们容易得知 $z+y$，$z-y$ 都是奇数的平方. 设 $z+y=u^2$，$z-y=v^2$，显然 $u>v$. 再我们把 u，v 写成

$$u=a+b,\qquad v=a-b,$$

这是可能的，因为我们取

$$a=\frac{u+v}{2},\quad b=\frac{u-v}{2}$$

就行了. 显然这时，$a>b>0$. 于是

$$z+y=(a+b)^2,\ z-y=(a-b)^2$$

因此

$$z=\frac{(a+b)^2+(a-b)^2}{2}=a^2+b^2,$$

$$y=\frac{(a+b)^2-(a-b)^2}{2}=2ab,$$

$$x=(a+b)(a-b)=a^2-b^2.$$

因为 $(z,\ x)=1$，并且 z，x 都是奇数，所以

$$(z+x,\ z-x)=2.$$

又因为 $z+x=2a^2$，$z-x=2b^2$，所以 $(a,\ b)=1$. 再因为 x 是奇数，所以 $a+b$ 是奇数，因此 a，b 一为奇数，一为偶数. 于是 a，b 满足定理中各条件.

定理证毕.

一般假如 $(x,\ y)=d$，那末 $(x,\ y,\ z)=d$，因此(1)的任意解可以表为

$$x=\pm d(a^2-b^2),\ y=\pm 2abd,\ z=\pm d(a^2+b^2).$$

例 1　求(1)中 $0<z<30$ 的所有互质的解.

解 由定理1，$a^2+b^2<30$，$a>b>0$，得$a\leqslant 5$．又因为a，b一为奇一为偶，求出a，b的值即得所求解，结果列表如下：

b	a	x	y	z
1	2	3	4	5
1	4	15	8	17
2	3	5	12	13
2	5	21	20	29
3	4	7	24	25

例 2 试证$x^2+2y^2=z^2$，$(x, y, z)=1$的整数解可以写成为

$$x=\pm(a^2-2b^2),\quad y=2ab,\quad z=a^2+2b^2.$$

证 因为$(x, z)=1$，所以$(z+x, z-x)=1$或2，又因为x，z只能同为奇数，所以$(z+x, z-x)=2$．于是$z+x$，$z-x$不能都是4的倍数．如果$z+x$不是4的倍数，那末$\frac{z+x}{2}$是奇数，因此$\left(\frac{z+x}{2}, z-x\right)=1$．由

$$y^2=\frac{z+x}{2}(z-x),$$

得知奇数$\frac{z+x}{2}$及偶数$z-x$都是平方数．设$\frac{z+x}{2}=a^2$，$z-x=(2b)^2$，因此得

$$x=a^2-2b^2,\quad y=2ab,\quad z=a^2+2b^2.$$

如果$z-x$不是4的倍数，那末由

$$y^2=(z+x)\frac{z-x}{2},$$

命 $z+x=(2b)^2$，$\frac{z-x}{2}=a^2$，即得

$$x=-(a^2-2b^2)，y=2ab，z=a^2+2b^2.$$

证毕.

例 3 试证 $x^{-2}+y^{-2}=z^{-2}$，$(x, y, z)=1$ 的正整数解可以表为

$$x=a^4-b^4，y=2ab(a^2+b^2)，z=2ab(a^2-b^2),$$

这里 $a>b>0$，$(a, b)=1$，a，b 一奇一偶.

证 充分性是显然的，仅证必要性. 因为 $(x,y,z)=1$，所以 $(x^2, y^2, z^2)=1$，于是由 § 1 例 5 得

$$x^2=r(r+s)，y^2=s(r+s)，z^2=rs,$$

这里 r，$s>0$，$(r, s)=1$. 由 $z^2=rs$，$(r,s)=1$ 得知 r，s 都是平方数，又由 $x^2=r(r+s)$ 得知 $r+s$ 也是平方数，令

$$r=r_1^2，s=s_1^2，r+s=t_1^2,$$

得 $$r_1^2+s_1^2=t_1^2，r_1，s_1>0，(r_1, s_1)=1$$

由定理 1 得

$$r_1=a^2-b^2，s_1=2ab，t_1=a^2+b^2$$

这里 $a>b>0$，$(a, b)=1$，a，b 一奇一偶，于是

$$x=r_1t_1=a^4-b^4,$$
$$y=s_1t_1=2ab(a^2+b^2),$$
$$z=r_1s_1=2ab(a^2-b^2).$$

证毕.

定理 2 假定 x,y，z 是(1)的解，并且 $(x, y, z)=1$，那末在 x，y 中有一是 3 的倍数，有一是 4 的倍数，在 x,y，z 中有一是 5 的倍数.

证明 假定 x，y 都不是3的倍数，因为不是3的倍数的数其形状是 $3n\pm1$，它们的平方

$$(3n\pm1)^2=3(3n^2\pm2n)+1=3k+1.$$

因此 x^2+y^2 的形状是 $3k-1$，它不是平方数，这与 z^2 是平方数矛盾．所以在 x，y 中必有一是3的倍数．

再假如 x，y 都不是4的倍数，因为不是4的倍数的数是 $4n\pm1$，$4n+2$，它们的平方

$$(4n\pm1)^2=8(2n^2\pm n)+1=8k+1,$$

$$(4n+2)^2=8k+4.$$

如果 x，y 都是形如 $4n\pm1$ 的数或一是 $4n\pm1$，一是 $4n+2$，那末 x^2+y^2 的形状是 $8k+2$ 或 $8k+5$，它们都不是平方数，这是矛盾．所以在 x，y 中必有一是4的倍数．

又假如 x，y，z 都不是5的倍数，那末它们的形状是 $5n\pm1$，$5n\pm2$，但

$$(5n\pm1)^2=5k+1,\ (5n\pm2)^2=5k-1$$

因此 x^2+y^2 的形状是 $5k-2$，$5k+2$ 或 $5k$，对前者 x^2+y^2 不是平方数，对后者 z 是5的倍数，这都与假设矛盾．所以，在 x，y，z 中必有一是5的倍数．

定理证毕．

要注意的是：定理中说在 x，y 中有一是3的倍数，有一是4的倍数，并不是说在 x，y 中一是3的倍数．另一是4的倍数，很可能3的倍数，4的倍数是同一个数．在上面例1中也有的就是如此．再如在 $11^2+60^2=61^2$ 中，11，61都是质数，只有60它是3的倍数，4的倍数，又同时是5的倍数，这时三个倍数是一个数．

最后我们介绍一个没有解决的古老难题．

1637 年法国数学家费马提出了下面一个猜想：

当 $n>2$ 时，方程 $x^n+y^n=z^n$ 没有正整数解．这就是有名的费马最后定理或费马大定理．我们知道一个大于 2 的整数必能被 4 或奇质数整除，因此，如果对 $n=4$ 或 n 等于任意奇质数都没有正整数解，那末问题就全部解决．但这个愿望还没有完全得到实现，下面我们来证明对于 $n=4$，这个猜想是正确的．

定理 3 方程 $x^4+y^4=z^2$ 没有正整数解．

证明 我们用反证法来证明，假定

$$(x^2)^2+(y^2)^2=z^2$$

有正整数解，这时我们不妨假定 $x>0$，$y>0$，$z>0$，y 是偶数，并且假定这时的 z 是所有解中 z 的最小值．由定理 1 得

$$x^2=a^2-b^2,\ y^2=2ab,\ z=a^2+b^2$$

这里 $(a, b)=1$，并且 a, b 一为奇，一为偶．如果 a 是偶数，那末 b 就是奇数，这时 $4n+1=x^2=a^2-b^2=4m-1$，此不可．所以 b 是偶数，于是由

$$x^2+b^2=a^2$$

根据定理 1，我们又得

$$x=p^2-q^2,\ b=2pq,\ a=p^2+q^2$$

这里 $(p, q)=1$，$p>q>0$，并且 p, q 一为奇一为偶．由 $y^2=2ab$，得

$$y^2=4pq(p^2+q^2).$$

因为 p, q, p^2+q^2 两两互质，所以它们都必是某数的平方，即

$$p=r^2,\ q=s^2,\ p^2+q^2=t^2$$

于是

$$r^4+s^4=t^2,$$

这时 $$z=a^2+b^2>a=t^2>t$$
这与 z 是最小值的假设矛盾，因此定理得证.

于是我们立即推得 $x^4+y^4=z^4$ 也没有正整解，因为如果它有正整数解，那末 $x^4+y^4=(z^2)^2$ 也就有正整数了，这显然是矛盾.

此外，$x^{-4}+y^{-4}=z^{-4}$ 也没有正整数解. 因为用 $(xyz)^4$ 乘两边就得到 $(yz)^4+(zx)^4=(xy)^4$，因为后者没有解，前者当然没有解.

例 4 试证 $x^n+1=y^{n+1}$ 没有正整数解，这里
$$n\geqslant 2,\quad (x,n+1)=1.$$

证 因为 $y-1$ 的质因数 p 能够整除 x，而 $(x,n+1)=1$，所以 $p\nmid(n+1)$，又因为
$$1+y+\cdots+y^n\equiv n+1\ (\mathrm{mod}\ (y-1)),$$
所以 $y-1$ 与 $1+y+\cdots+y^n$ 互质，于是由
$$x^n=(y-1)(1+y+\cdots+y^n)$$
得知 $1+y+\cdots+y^n$ 是某数的 n 次方，这是矛盾. 因为
$$y^n<1+y+\cdots+y^n<(y+1)^n.$$
所以例成立.

费马大定理经过多少数学家的努力，到现在还是没有完全得到证实，1978 年，瓦格斯塔夫 (Wagstaff) 在大型计算机帮助下证明当 $2<n<125000$ 时定理是正确的. 在 x，y，z 与 n 互质的情况下，现在只知道 $x<253,747,889$ 时定理是正确的，即 $x^n+y^n=z^n$ 没有正整数解.

习 题 3．2

1．求(1)中 $0<z<60$ 的所有互质的解.

2. 求三个整数 $x>y>z>0$ 使 $x-y$, $y-z$, $x-z$ 都是平方数.

3. 假如 $p=4k-1$, 试证 p 不能表为二个平方数的和.

4. 求使 x^2-60 为平方数的 x.

5. 试求使 $t-5$ 及 $t+5$ 都是平方数的平方数 t.

6. 求 $x^2-y=y^2+x-18$ 的正整数解.

7. 试证不定方程 $x^4-4y^4=z^2$ 没有正整数解.

8. 试证不定方程 $x^2-3y^n=-1$, n 是正整数, 没有正整数解.

9. 试证每个正整数n可以写成

$$n=x^2+y^2-z^2$$

这里 x, y, z 都是整数.

10. 试证不论 n 为何正整数, $x^2+y^2=z^n$ 总有整数解.

11. 假设 n 是正整数, 试证

$$(2n^2+n)^2+(2n^2+n+1)^2+\cdots+(2n^2+2n)^2$$
$$=(2n^2+2n+1)^2+(2n^2+2n+2)^2+\cdots+(2n^2+3n)^2,$$

因而求 $$x_1^2+x_2^2+x_3^2+x_4^2=x_5^2+x_6^2+x_7^2$$

的一组正整数解.

§3.3 两个平方数的和

上节定理 1 是解毕达哥拉斯不定方程, 但同时也说明怎样的平方数可以写成两个平方数的和. 任意正整数不一定能够写成两个平方数的和, 譬如 $10=1^2+3^2$, $13=2^2+3^2$ 但 6,7 就不行.

我们讨论的 (或者除本节外) 都是所谓的乘法数论的内

容，因为它的基本运算是乘法，大多数定理都是关于数的可约性的以及一数表为积的形状的．整个同余理论基本上可以看成是可约性比较复杂的情况．假如用加法来代替乘法，即加法起基本作用，得到的结果就是加法数论或者是堆垒数论，它比乘法数论更为复杂，当然彼此还是有联系的．

在加法数论中，刁番图有一个著名的猜想：一个正整数可以写成 4 个平方数的和．1636 年费马已知道证法，但第一次公布其证法的是 1770 年拉格朗日（J. L. Lagrange，1736～1813）．1770年华林（E. Waring，1734～1798）更作如下的猜想：任意正整数可以写成 4 个平方数的和，9 个立方数的和，19 个四方数的和．百余年后，1909 年，希尔伯特（D. Hilbert，1862～1943）证明了下面比它更广泛的结论：

对于任意整数 $k\geqslant 2$，存在一个正整数 $r=r(k)$，使得任意正整数 N 可以表为

$$N=x_1^k+x_2^k+\cdots+x_r^k,$$

这里整数 $x_i\geqslant 0$．

这节我们只讨论那些数可以写成两个平方数的和，首先我们有：

定理 1 形如 $4n-1$ 的数不能表为两个平方数的和

证明 设 m 为正数，并且 $m\equiv -1(\mathrm{mod}4)$，如果

$$m=x^2+y^2,$$

因为对于模 4，x，y 只与 0，1，2，-1 等同余，所以 x^2，y^2 只能与 0，1 同余，因此

$$x^2+y^2\equiv 0，1 或 2(\mathrm{mod}\ 4),$$

这与 $m\equiv -1(\mathrm{mod}4)$ 的假设不合，于是定理成立．

再讨论形如 $4n+1$ 的质数．先证明下面两个性质以备引

用.

定理 2 假定质数 $p=4n+1$，$q=\frac{1}{2}(p-1)$，$b=q!$，那末

$$b^2+1\equiv 0(\bmod p).$$

证明 因为最前的 $p-1$ 个正整数可以写成

$$1,\ 2,\ \cdots,\ q,\ p-q,\ p-(q-1),\ \cdots p-1$$

所以我们有

$$1\equiv 1(\bmod p),\quad \cdots,\quad q\equiv q(\bmod p)$$

$$p-q\equiv -q(\bmod p),\ \cdots,\ p-1\equiv -1(\bmod p).$$

把这 $p-1$ 个同余式相乘得

$$(p-1)!\equiv(-1)^q(q!)^2(\bmod p).$$

因为 p 是质数，由威尔生定理（§ 4.2 定理 3），得

$$(-1)^q(q!)^2\equiv -1(\bmod p)$$

即
$$b^2\equiv(-1)^{q+1}\ (\bmod p)$$

但 $p=4n+1$，所以 $q=2n$，因此 $q+1=2n+1$，于是

$$b^2\equiv -1\ (\bmod p)$$

定理成立.

譬如 $p=13$ 时，$q=6$，$6!=720$，于是

$$(720)^2+1=518401=13\times 39877\equiv 0(\bmod p).$$

定理 3 假定 p 是质数，r 是满足 $r^2>p$ 的最小正数，n 是与 p 互质的整数，即 $(n,\ p)=1$，那就有小于 r 的正整数 a，c 存在，使得

$$n^2a^2\equiv c^2(\bmod p)$$

证明 设 $M=\{nx-y|\ x,\ y$ 是小于 r 的非负整数$\}$，显然 M 包含 r^2 个数，因此其中有 nx_1-y_1，nx_2-y_2 关于 p 同

余，即

$$nx_1 - y_1 \equiv nx_2 - y_2 \pmod p$$

于是 $$n(x_1 - x_2) \equiv y_1 - y_2 \pmod p$$

所以 $$n^2(x_1 - x_2)^2 \equiv (y_1 - y_2)^2 \pmod p$$

如果 $x_1 = x_2$，那末 $y_1 \equiv y_2 \pmod p$，因为 $r < p$(当 $p \geqslant 3$ 时 $p^2 - 3p + 1 > 0$，即 $(p-1)^2 > p$) 所以 $y_1 = y_2$，如果 $y_1 = y_1$，那末 $n(x_1 - x_2) \equiv 0 \pmod p$ 因为 $(n, p) = 1$，所以 $x_1 \equiv x_2 \pmod p$. 因此 $x_1 = x_2$，这就是说 $|x_1 - x_2| \neq 0$，$|y_1 - y_2| \neq 0$. 于是命 $a = |x_1 - x_2|$，$c = |y_1 - y_2|$ 就得到我们求证的等式. 所以定理成立.

譬如 $p = 13$ 时，$r = 4$，如果取 $n = 5$，我们容易得知

$$25a^2 \equiv c^2 \pmod{13}$$

显然 $a = 2$，$c = 3$ 时上式成立.

有了上面两个性质，下面的主要定理就容易证明了

定理 4 形如 $4n+1$ 的质数能够表为两个平方数的和.

证明 由定理 3，我们有

$$n^2a^2 \equiv c^2 \pmod p$$

取 n 为定理 2 中的 b 即 $n = b$，因为 $b^2 \equiv -1 \pmod p$. 所以

$$-a^2 \equiv c^2 \pmod p$$

即 $$a^2 + c^2 = kp$$

但 $0 < a^2 < p$，$0 < c^2 < p$，所以

$$0 < a^2 + c^2 < 2p$$

因此 $$a^2 + c^2 = p$$

定理证毕.

因为 $2 = 1^2 + 1^2$，又奇数的形状不是 $4n-1$ 便是 $4n+1$，于是由上面定理我们又得.

定理 5 不是形如 $4n-1$ 的质数都能表为两个平方数的和.

假如 $m=a^2+b^2$，显然 $r^2m=(ra)^2+(rb)^2$. 又假如 $n=c^2+d^2$，那末

$$
\begin{aligned}
mn &= (a^2+b^2)(c^2+d^2)=a^2c^2+b^2d^2+a^2d^2+b^2c^2\\
&= (a^2c^2+b^2d^2\pm 2abcd)+(a^2d^2+b^2c^2\mp 2abcd)\\
&= (ac\pm bd)^2+(ad\mp bc)^2
\end{aligned}
$$

这就是说，一个能表为两个平方数和的数与一个平方数的乘积，仍然是一个两个平方数和的数. 两个能表为两个平方数和的数的乘积，也是一个两个平方数和的数.

于是，我们得知一个正整数，如果它的非平方的质因数都是 $4n+1$ 的形状，那末这整数可以表为两个平方数的和. 譬如

$$
\begin{aligned}
m &= 585=3^2\cdot 5\cdot 13=3^2(1^2+2^2)(2^2+3^2)\\
&= 3^2\{(2+6)^2+(3-4)^2\}=3^2(8^2+1^2)\\
&= 24^2+3^2.
\end{aligned}
$$

下面是这性质的逆.

定理 6 假定 m 是正整数，$m=r^2m'$，并且 m' 的因数不是平方数，那末 m 能够表为两个平方数和的必要充分条件是 m' 没有形如 $4n-1$ 的质因数.

证明 充分性已如上述，下面用反证法来证明必要性.

假定 m' 有形如 $4n-1$ 的质因子 p，并且

$$m=r^2m'=x^2+y^2.$$

由定理 4 的证明，我们容易得知只要求得 $n^2+1\equiv 0(p)$，那末 p 就是两个平方数的和，这与定理 1 矛盾，于是必要条件成立. 下面我们来求这样的 n.

设$(x, y)=d$，$x=dx'$，$y=dy'$，$(x', y')=1$，那末

$$x'^2+y'^2=\left(\frac{r}{d}\right)^2 m'$$

因为m'没有平方因数，所以$\frac{r}{d}$是整数，即$r=dr'$，于是

$$x'^2+y'^2=r'^2m'$$

因为$(x', y')=1$，所以x'，y'中最少有一必须与p互质. 设$(x', p)=1$，根据§2.2费马小定理，有s使

$$sx'\equiv 1 \pmod p$$

于是 $$s^2(x'^2+y'^2)=(sx')^2+(sy')^2\equiv 0 \pmod p$$

即 $$(sy')^2+1\equiv 0 \pmod p$$

这样我们就得到所求的$n=sy'$. 定理证毕.

要注意的是一个数如果能够表为两个平方数的和，其表示法一般不是唯一的. 譬如

$$125=10^2+5^2=11^2+2^2,\quad 325=18^2+1^2=17^2+6^2$$

但质数的表示是唯一的，这就是下定理：

定理 7 质数表为两个平方数和的方法是唯一的.

证明 假定质数$p=a^2+b^2=c^2+d^2$，于是

$$\begin{aligned}p^2&=(a^2+b^2)(c^2+d^2)\\&=(ac+bd)^2+(ad-bc)^2\\&=(ac-bd)^2+(ad+bc)^2\end{aligned}\tag{1}$$

又 $$\begin{aligned}(ac+bd)(ad+bc)&=(a^2+b^2)cd+(c^2+d^2)ab\\&=p(ab+cd)\end{aligned}$$

所以 $$p\mid(ac+bd)\text{ 或 }p\mid(ad+bc).$$

如果$p\mid(ac+bd)$，那末$ac+bd=kp$，代入(1)式得

$$p^2=k^2p^2+(ad-bc)^2$$

因此$ad-bc=0$，即$a=rc$，$b=rd$，所以

$$a^2+b^2=r^2(c^2+d^2)$$

于是 $r=1$，这就是说 $a=c$，$b=d$.

如果 $p|(ad+bc)$，那末 $ad+bc=kp$，代入(1)式右边，同上面一样，我们有 $a=rb$，$d=rc$. 于是

$$(r^2+1)b^2=(1+r^2)c^2,$$

所以 $b=c$，也就是 $b=c$，$a=d$.

定理证毕.

于是一个数表为两个平方数和的方法如果不是唯一的，那末这数就是合数.

同上面一样，有的数可以表为 3 个平方数的和，有的数不能这样表示，但任意数可以表为 4 个平方数的和，这些我们都不详细论证了. 下面举两例结束本节.

例 1 设 $n\equiv 7 \pmod 8$，那末 n 不能表为 3 个平方数的和.

证 用反证法，假如

$$n=x^2+y^2+z^2,$$

那末
$$7\equiv x^2+y^2+z^2 \pmod 8$$

因此，x，y，z 中必定有一是奇数. 假定 x 是奇数，由 $x^2\equiv 1 \pmod 8$ 我们有 $6\equiv y^2+z^2 \pmod 8$，因此 y，z 同为奇数或同为偶数，同为奇数显然不成立. 同为偶数，如果 y 是偶数，由 $y\equiv 4 \pmod 8$，上式也同样不成立. 所以例成立.

例 2 两个 4 个平方数之和的乘积仍是 4 个平方数的和.

证 由下等式即得.

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)$$
$$=(ae+bf+cg+dh)^2+(af-be+ch-dg)^2$$

$$+(ag-bh-ce+df)^2+(ah+bg-cf-de)^2$$

这结果是1743年欧拉提出的，欧拉经过一个较长时间才得到上等式证明这性质．假如没有这等式，这个简单性质还是不容易证明的．

习 题 3．3

1．把下列各数写成两个平方数的和(如可能)

365， 1105， 1961， 5461

2．假如 $8\mid(a^2+b^2+c^2+d^2)$，那末 a，b，c，d 都是偶数．

3．证明正整数 m 能够表为两个平方数的差，即

$$m=a^2-b^2,$$

的必要充分条件是 m 能够表为两个因数的乘积，这两因数同为偶数或同为奇数．

4．试证任意整数的立方是两个平方数之差．

5．假如 $n=a^2+b^2=c^2+d^2$，试证

$$n=\frac{\{(a-c)^2+(b-d)^2\}\{(a+c)^2-(b-d)^2\}}{4(b-d)^2},$$

这就是说一个数如果能够用两种不同的方式表为两个平方数的和，那末它就是合数．

6．三个相邻数其中有两数是两个平方数的和，试证这样三个数的数组有无穷多组．

7．求所有适合 $x^3+y^3+z^3=w^3$ 并成几何级数的正整数 x，y，z，w．

第四章 一元同余方程

在代数中，求解方程是一个重要问题. 在这里，求解同余方程也是一个重要问题.

一元同余方程

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \pmod{m},$$

当 $m \nmid a_0$ 时，叫做 n 次同余方程. 使 $f(\alpha) \equiv 0 \pmod{m}$ 的数 α，叫做它的解，或根. 二个对 m 不同余的解，叫做**不相同的**解. 这章讨论解 $f(x) \equiv 0 \pmod{m}$，，也就是讨论它是否有解，假如有解，有多少个解，又如何去求解等问题.

§4.1 一次同余方程

一元一次同余方程一般的形状是

$$ax + b \equiv 0 \pmod{m}, \tag{1}$$

我们分二种情况来讨论它的解.

1. $(a, m) = 1$.

假定 $x_1, x_2, \cdots, x_m$ 是 m 的完全剩余系，因为 $(a, m) = 1$，由§2.2定理2，$ax_1 + b, ax_2 + b, \cdots, ax_m + b$ 也是 m 的完全剩余系，因此其中必有一数而且只有一数与零同余，即 $ax_k + b \equiv 0 \pmod{m}$，这就是说(1)有解并且只有唯一个解，再由(1)我们有

$$ax \equiv -b \pmod{m},$$

因为$a^{\varphi(m)}\equiv 1 \pmod m$，所以

$$a^{\varphi(m)}x\equiv -a^{\varphi(m)-1}b \pmod m,$$

即
$$x\equiv -a^{\varphi(m)-1}b \pmod m$$

是(1)的解.

2. $(a, m)=d>1$.

假如(1)有解，那末$d\mid b$，反过来假如$d\mid b$，因为$\left(\frac{a}{d}, \frac{m}{d}\right)=1$，所以

$$\frac{a}{d}x+\frac{b}{d}\equiv 0\left(\bmod \frac{m}{d}\right) \tag{2}$$

有解，因此(1)也有解．显然(1)与(2)等价，也就是说(1)的解都是(2)的解，反过来(2)的解也都是(1)的解，这样求解(1)我们只要求解(2)就行了．但要注意的是(1)，(2)两方程的模不同，(2)的相同的解不一定也就是(1)的相同的解，下面我们在(2)的所有解中来求出(1)的所有不相同的解.

假定(2)的唯一解为$x\equiv\alpha\left(\bmod \frac{m}{d}\right)$，那末所有形状象$\alpha+t\frac{m}{d}$，$t$是任意整数，的数都是(2)的解，因此这些数中所有关于模m不同余的数就是(1)的所有解．因为当

$$\alpha+t_1\frac{m}{d}\equiv\alpha+t_2\frac{m}{d} \pmod m \tag{3}$$

时，我们有$\frac{t_1-t_2}{d}m\equiv 0 \pmod m$，于是$t_1\equiv t_2 \pmod d$，反过来也成立．这就是说(3)成立的必要充分条件是$t_1\equiv t_2 \pmod d$．因此在所有形状象$\alpha+t\frac{m}{d}$的数中只要t取关于模d不同余的数得到的数就关于模m不同余．所以

$$a,\ a+\frac{m}{d},\ \cdots,\ a+(d-1)\ \frac{m}{d}$$

就是(1)的所有解，于是我们有：

定理 1 一元一次同余方程(1)当$(a, m)=1$时，有唯一解

$$x\equiv -a^{\varphi(m)-1}b\ (\mathrm{mod}\ m),$$

当$(a, m)=d>1$时，(1)有解的必要充分条件是$d\mid b$，这时(1)有d个解

$$x\equiv a+t\frac{m}{d}\ (\mathrm{mod}\ m),\qquad t=0,\ 1,\ \cdots,\ d-1$$

这里$x\equiv a\left(\mathrm{mod}\ \frac{m}{d}\right)$是(2)的唯一解.

在实际求解时，我们不常用公式，因为用公式一般比较麻烦.

例 1 解 $12x+15\equiv 0\ (\mathrm{mod}\ 45)$.

解 因为$(12, 45)=3\mid 15$，所以同余方程有解，并且有3个解，用视察法解同余方程

$$4x+5\equiv 0\ (\mathrm{mod}15),$$

得
$$x\equiv -5\equiv 10\ (\mathrm{mod}\ 15),$$

因此所求的三个解为

$$x\equiv 10,\ 10+15,\ 10+30\ (\mathrm{mod}45),$$

即

$$x\equiv 10,\ 25,\ 40\ (\mathrm{mod}\ 45).$$

例 2 解 $103x\equiv 57\ (\mathrm{mod}\ 211)$.

解 这时103，211都是质数，所以同余方程只有唯一个解.

因为$211=2\cdot 103+5$，用2乘所给式两边得

$$206x \equiv 114 \pmod{211}.$$

再由 $211x \equiv 0 \pmod{211}$ 与上式相减得

$$5x \equiv -114 \equiv 97 \pmod{211},$$

又因为 $211 = 42 \cdot 5 + 1$，所以

$$42 \cdot 5x \equiv 42 \cdot 97 \equiv 65 \pmod{211},$$

即
$$x \equiv -65 \pmod{211}.$$

是所求解．解毕．

从(1)我们有 $ax + b = my$ 即 $ax + m(-y) = -b$，反过来也成立．因此，解同余方程有时用不定方程求解比较方便．

例 3 **解** $111x \equiv 75 \pmod{321}$.

解 因为 $(111, 321) = 3 | 75$，所以同余方程有三个解．把所给同余方程化为

$$37x \equiv 25 \pmod{107}$$

解不定方程

$$37u + 107v = 25 \tag{*}$$

得 $u = -8$，$v = 3$，于是

$$x \equiv -8 \equiv 99 \pmod{107}$$

是(*)的解，因此所求的 3 个解为

$$x \equiv 99,\ 99 + 107 = 206,\ 99 + 214 = 315,\ \pmod{321}.$$

再从(1)我们有 $my \equiv -b \pmod{a}$，假如 y_0 是它的解，那末

$$x_0 = \frac{my_0 - b}{a}$$

就是(1)的解了，求解此式有时比解(1)方便．

例 4 **解** $863x \equiv 880 \pmod{2151}$

解 由原式得

$$2151y \equiv -880 \pmod{863}$$

即 $425y \equiv -880 \pmod{863}$

用5除两边得 $85y \equiv -176 \pmod{863}$

又 $863z \equiv 176 \pmod{85}$

即 $13z \equiv 6 \pmod{85}$

再 $85\omega \equiv -6 \pmod{13}$

即 $7\omega \equiv -6 \pmod{13}$

因此 $\omega_0 = 1$

于是 $z_0 = \dfrac{85+6}{13} = 7$

$$y_0 = \frac{863 \times 7 - 176}{85} = 69$$

$$x_0 = \frac{2151 \times 69 + 880}{863} = 173$$

即 $x \equiv 173 \pmod{2151}$是所求解，因为$(863, 2151) = 1$，所以所给方程只有这唯一解．解毕．

多元一次同余方程我们可以化为一元一次同余方程来求解．

例 5 解 $2x + 7y \equiv 5 \pmod{12}$.

解 所给方程可以写成

$$2x \equiv 5 - 7y \pmod{12}.$$

因为$(2, 12) = 2$，于是我们有

$$7y \equiv 5 \pmod{2}.$$

解之得 $y \equiv 1 \pmod{2}$，

或 $y = 1 + 2t$.

代入所给方程得

$$2x \equiv -2-14t \pmod{12},$$

即 $$x \equiv -1-7t \pmod{6}$$

因此 $$x = -1-7t+6s.$$

于是所求的全部解 $y \equiv 1+2t$，$x \equiv -1-7t+6s \pmod{12}$，这里 $t=0, 1, \cdots, 5$；$s=0, 1$，共 12 组解，即

$$\begin{cases}x\equiv 5\\ y\equiv 1,\end{cases}\quad \begin{cases}x\equiv 11\\ y\equiv 1,\end{cases}\quad \begin{cases}x\equiv 4\\ y\equiv 3,\end{cases}\quad \begin{cases}x\equiv 10\\ y\equiv 3,\end{cases}$$

$$\begin{cases}x\equiv 3\\ y\equiv 5,\end{cases}\quad \begin{cases}x\equiv 9\\ y\equiv 5,\end{cases}\quad \begin{cases}x\equiv 2\\ y\equiv 7,\end{cases}\quad \begin{cases}x\equiv 8\\ y\equiv 7,\end{cases}$$

$$\begin{cases}x\equiv 1\\ y\equiv 9,\end{cases}\quad \begin{cases}x\equiv 7\\ y\equiv 9,\end{cases}\quad \begin{cases}x\equiv 0\\ y\equiv 11,\end{cases}\quad \begin{cases}x\equiv 6\\ y\equiv 11,\end{cases}$$

下面我们来讨论一次同余方程组的解.

在代数方程中，二个不同的一元一次方程没有公共解，也就是说在代数方程中没有一元一次方程组的求解问题. 但对于模不同的一元一次同余方程组不是这样，因为模不同，所以求它们的解就变成有意义的问题了.

我们先就模是互质的简单情况来讨论. 下面的定理叫做**孙子定理**是早在三世纪我国孙子提出的，这就是中外驰名的所谓中国剩余定理.

定理 2 假定 m_1，m_2，$\cdots$，m_k 两两互质，那末同余方程组

$$\begin{cases}x\equiv a_1 \pmod{m_1}\\ \cdots\cdots\cdots\cdots\\ x\equiv a_k \pmod{m_k}\end{cases} \tag{4}$$

对于模 $m=m_1m_2\cdots m_k$ 有唯一解

$$x \equiv \frac{m}{m_1}x_1a_1 + \cdots + \frac{m}{m_k}x_ka_k \pmod{m},$$

这里 $$\frac{m}{m_i}x_i \equiv 1 \pmod{m_i}.$$

证明 因$\left(\frac{m}{m_i}, m_i\right)=1$,所以同余方程$\frac{m}{m_i}x \equiv 1 \pmod{m_i}$有唯一个解 x_i,即

$$\frac{m}{m_i}x_i \equiv 1 \pmod{m_i}.$$

这时显然 $$\frac{m}{m_i}x_i \equiv 0 \pmod{m_j},\ i \neq j,$$

设 $$\alpha = \frac{m}{m_1}x_1a_1 + \cdots + \frac{m}{m_k}x_ka_k,$$

于是 $\alpha \equiv a_i \pmod{m_i}$,所以 $x \equiv \alpha \pmod{m}$ 是(4)的解.

再假如 $\beta \equiv a_i \pmod{m_i}$ 又是(4)的解,那末 $\alpha \equiv \beta \pmod{m_i}$,因为$(m_i, m_j)=1$,所以 $\alpha \equiv \beta \pmod{m}$ 这就是说对于模 m,(4)只有唯一个解,因此定理成立.

例 6[①] 解同余方程组

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

解 解同余方程

$35x \equiv 1 \pmod{3}$, $21x \equiv 1 \pmod{5}$, $15x \equiv 1 \pmod{7}$

---

① 此即孙子算经书中提出的问题之一.今有物不知其数,三三数之剩二,五五数之剩三,七七数之剩二,问物几何?答曰二十三,关于它的一般解法,明朝程大位的算经统宗(1593)书中有一歌诀:

三人同行七十希,五树梅花廿一枝,

七子团圆整半月,除百零五便得知.

得　　　$x_1\equiv 2\pmod 3$，$x_2\equiv 1\pmod 5$，$x_3\equiv 1\pmod 7$，

于是所求解

$$x\equiv 35\cdot 2\cdot 2+21\cdot 1\cdot 3+15\cdot 1\cdot 2$$
$$=233\equiv 23\pmod{105}.$$

例 7　解

$$\begin{cases}2x\equiv 1 \pmod 5\\ 3x\equiv 4 \pmod 7\end{cases},$$

解　解 $2x\equiv 1\pmod 5$ 得 $x\equiv 3\pmod 5$，解 $3x\equiv 4\pmod 7$ 得 $x\equiv 6\pmod 7$，于是所给同余方程组与同余方程组

$$\begin{cases}x\equiv 3 \pmod 5\\ x\equiv 6 \pmod 7\end{cases} \qquad (*)$$

等价. 命 $x=3+5y$，那末 $3+5y\equiv 6\pmod 7$，即 $5y\equiv 3\pmod 7$，显然 $y\equiv 2\pmod 7$，因此所求解为

$$x=3+5y\equiv 3+10\equiv 13\pmod{35}.$$

我们也可以这样来求解. 由(*)得

$$x=3+5y=6+7z$$

即　　　$$5y-7z=3,$$

显然　$y=2$，$z=1$，所以

$$x=3+10=6+7=13.$$

再我们来讨论模不互质的同余方程组. 它们的解我们也可以同样求得

例 8　解

$$\begin{cases}x\equiv -2 \pmod{12}\\ x\equiv 6 \pmod{10}\\ x\equiv 1 \pmod{15}\end{cases}$$

解　原方程组可以化为

$$\begin{cases} x \equiv -2 \pmod{2^2} \\ x \equiv -2 \pmod{3} \\ x \equiv 6 \pmod{2} \\ x \equiv 6 \pmod{5} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5}, \end{cases}$$

因为由

$$\begin{cases} x \equiv -2 \pmod{2^2} \\ x \equiv 6 \pmod{2}, \end{cases} \quad 得 \ x \equiv -2 \pmod{2^2};$$

$$\begin{cases} x \equiv -2 \pmod{3} \\ x \equiv 1 \pmod{3}, \end{cases} \quad 得 \ x \equiv 1 \pmod{3};$$

$$\begin{cases} x \equiv 6 \pmod{5} \\ x \equiv 1 \pmod{5}, \end{cases} \quad 得 \ x \equiv 1 \pmod{5};$$

于是我们有

$$\begin{cases} x \equiv -2 \pmod{2^2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

用孙子定理求解，得所求解

$$x \equiv 46 \pmod{60}.$$

下面是同余方程组有解的必要充分条件.

定理 3 同余方程组

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \tag{5}$$

有解的必要充分条件是

$$a \equiv b \pmod{(m, n)}.$$

假如这条件成立，那末(5)对于模$[m, n]$只有唯一解.

证明 假定 $x=c$ 是它的一个解，即

$$c\equiv a \pmod m, \quad c\equiv b \pmod n$$

于是 $a\equiv b(\bmod (m, n))$，所以必要条件成立.

再假如 $a\equiv b(\bmod (m, n))$，由定理1得知同余方程

$$my\equiv b-a \pmod n$$

有解 $y\equiv d(\bmod n)$. 于是下列两式成立

$$a+md\equiv a \pmod m, \quad a+md\equiv b(\bmod n)$$

即所给方程组有解 $x\equiv a+md$. $(\bmod [m, n])$ 所以充分条件也成立.

假如 x, y 都是同余方程(5)的解，那末

$$x\equiv y \pmod m, \quad x\equiv y(\bmod n),$$

因此 $x-y$ 是 m, n 的公倍数，当然也是$[m, n]$的倍数，于是 $x\equiv y(\bmod [m, n])$.

定理证毕.

一般我们有同余方程组

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

有解的必要充分条件是

$$a_i\equiv a_j(\bmod (m_i, m_j)), \quad i, j=1,\cdots,k$$

假如这条件成立，那末它对于$[m_1, \cdots, m_k]$只有唯一解.

习 题 4.1

1. 解下列一次同余方程

   1) $256x\equiv 179(\bmod 337)$

   2) $1215x\equiv 560(\bmod 2755)$

3) $6x+15y\equiv 9 \pmod{18}$

2. 试用同余方程解法求解不定方程 $37x+49y=1$.

3. 解同余方程组

$$\begin{cases} x\equiv 1 \pmod 4 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7 \end{cases}$$

4. 解同余方程组

$$1)\ \begin{cases} 5x\equiv 7 \pmod{11} \\ 6x+9\equiv 0 \pmod{19}, \end{cases}$$

$$2)\ \begin{cases} 4x\equiv 6 \pmod{14} \\ 9x\equiv 15 \pmod{33} \end{cases}$$

5. 解同余方程组

$$\begin{cases} 4x-3y+7z\equiv 5 \pmod{17} \\ 5x+y-3z\equiv 2 \pmod{17} \\ x-4y-z\equiv 1 \pmod{17} \end{cases}$$

6. 求一个最小的正 4 位数，它用 11 除余1，用 13 除余3，用 17 除余 7 .

7. 设 $m=p_1^{m_1}\cdots p_n^{m_n}$，$p_1$，$\cdots$，$p_n$ 是不同的质数，那末

$$x\equiv a \pmod m$$

与同余方程组

$$x\equiv a \pmod{p_1^{m_1}},\ \cdots,\ x\equiv a \pmod{p_n^{m_n}}$$

等价.

§4.2　质数模的高次同余方程

一般质数模同余方程

$$f(x)=a_0x^n+\cdots+a_n\equiv 0 \pmod p,\quad p\nmid a_0. \tag{1}$$

我们要求出它的解，并不是不可能，这只要把 p 的完全剩余系 0，±1，…，$\pm\frac{1}{2}(p-1)$ 中各数一一代入验证就可求得全部解．只是当 p 过大而尤其是 n 过大时，代入验算，显然不是一件轻而易举的事．但是舍此外，我们还没有一般的简便方法，为了减少计算上的困难，我们可以先进行如下的简化．

首先假如(1)中 $f(x)$ 的系数有大于 p 的都把它们化为小于 p．再如果 $f(x)$ 的次数 n 不小于 p，我们可以用 x^p-x 除 $f(x)$ 得到次数小于 p 的 $r(x)$：

$$f(x)=(x^p-x)q(x)+r(x),$$

或者说利用 $x^p\equiv x \pmod p$ 把 $f(x)$ 化为次数小于 p 的 $r(x)$，即

$$f(x)\equiv r(x) \pmod p,$$

显然 $f(x)$ 的不相同解与 $r(x)$ 的不相同解是一致的．因此解(1)的问题就变成解 $r(x)\equiv 0 \pmod p$ 的问题，因为 $r(x)$ 的次数比 $f(x)$ 的低，所以计算较简便．

再假如 $f(x)\equiv g_1(x)g_2(x) \pmod p$，那末求解(1)，就变成求解

$$g_1(x)\equiv 0 \pmod p \text{ 或 } g_2(x)\equiv 0 \pmod p.$$

因为 $g_1(x)$，$g_2(x)$ 的次数都比 $f(x)$ 的低，所以计算困难可

以大大减少.

又假如已知 $x\equiv a \pmod p$ 是(1)的解，由 $f(x)=(x-a)g(x)+r$，我们有 $r\equiv 0 \pmod p$，因此 $f(x)\equiv(x-a)g(x) \pmod p$，于是解(1)的问题就变为解 $g(x)\equiv 0 \pmod p$ 的问题，这时次数降低，计算简化了.

要重复的是(1)只有用数代入试验来求其解，这是解(1)的基本方法,上面的简化对某些个别方程也能行之有效,但不是一般都需要.

例 1 解 $f(x)=x^7-2x^6-7x^5+x+2\equiv 0 \pmod 5$

解 简化同余方程得

$$r(x)=x^3-2x^2-x+2\equiv 0 \pmod 5.$$

用 5 的完全剩余系 $-2,-1,0,1,2$ 代入，得知它有 3 个解

$$x\equiv -1,\ 1,\ 2 \pmod 5.$$

例 2 假设 p 是质数,那末同余方程 $x^{p-1}-1\equiv 0 \pmod p$ 有 $p-1$ 个解.

解 由费马定理，任意与 p 互质的数都是它的解，因此它有 $p-1$ 个不相同的解.

$$x\equiv 1,\ 2,\ \cdots,\ p-1 \pmod p.$$ 证毕.

假如 $p>2$ 由

$$x^{p-1}-1=(x-1)(x^{p-2}+x^{p-3}+\cdots+x+1),$$

得知 $p-2$ 次同余方程

$$x^{p-2}+x^{p-1}+\cdots+x+1\equiv 0 \pmod p$$

有 $p-2$ 个不相同的解：

$$x\equiv 2,\ 3,\ \cdots,\ p-1 \pmod p$$

同在代数方程中一样，假如关于模 p，$(x-a)^k$ 是 $f(x)$ 的因式，但 $(x-a)^{k+1}$ 不是 $f(x)$ 的因式，那末 $x\equiv a \pmod p$

叫做同余方程 $f(x)\equiv 0 \pmod p$ 的 k 重解．当 $k=1$ 时又叫做单解，当 $k>1$ 时叫做重解．

譬如在上例 1 中 $f(x)$ 可以写成

$$f(x)=(x^5-x)(x^2-2x-2)+(x^3-2x^2-x+2)$$
$$\equiv(x-1)(x+1)^2(x-2)^2(x^2+x+2) \pmod 5$$

因此 $x\equiv 1$ 是 $f(x)\equiv 0 \pmod 5$ 的单解，$x\equiv -1$，$2 \pmod 5$ 是重解，这三个解都是 $r(x)\equiv 0 \pmod 5$ 的单解．由这我们也可以看出虽然 $f(x)\equiv 0 \pmod p$ 与 $r(x)\equiv 0 \pmod p$ 的不相同的解是一致的，但它们在各方程中的重数不一定一致．

关于（1）的解的个数，我们有下面拉格朗日定理：

定理 1 (1) 的不相同解的个数不大于 $f(x)$ 的次数 n．

证明 我们用数学归纳法来证明．

$n=1$ 时，定理显然成立，假定 $n-1$ 时定理成立，假如 $x=a$ 是(1)的一个解，即 $f(a)\equiv 0 \pmod p$，命

$$f(x)\equiv(x-a)g(x) \pmod p$$

如果 $x\equiv b \pmod p$ 是(1)的任一解，我们就有

$$f(b)\equiv(b-a)g(b)\equiv 0 \pmod p,$$

因此 $b\equiv a \pmod p$ 或 $g(b)\equiv 0 \pmod p$，前者 b 与 a 同余，后者 $x\equiv b \pmod p$ 是 $g(x)\equiv 0 \pmod p$ 的解，也就是说(1)的解或是 $x\equiv a \pmod p$ 或是 $g(x)\equiv 0 \pmod p$ 的解，但 $g(x)$ 的次数是 $n-1$，根据假设它的不相同的解不多于 $n-1$ 个，因此(1)的解不多于 n 个，所以定理成立．

于是我们得知假如

$$a_0x^n+a_1x^{n-1}+\cdots+a_n\equiv 0 \pmod p$$

有多于 n 个不相同的解，那末它的所有系数都能用 p 整除，即

$$a_i \equiv 0 \pmod p,\ i=0,\ 1,\ \cdots,\ n.$$

要注意的是上定理只说明(1)的解个数的上限，但(1)的解的确切个数并不存在，譬如3次同余方程

$$x^3+4x^2+x+1\equiv 0 \pmod 5,$$
$$x^3+2x^2-2x+1\equiv 0 \pmod 5,$$
$$x^3-2x^2-x+2\equiv 0 \pmod 5$$

分别是没有解，有一个解 $x\equiv -2 \pmod 5$，有三个解 $x\equiv 1,\ -1,\ 2 \pmod 5$，再要注意的是上定理所以能够成立是模是质数，假如模是合数，定理不一定成立，譬如3次同余方程

$$x^3-x=x(x-1)(x+1)\equiv 0 \pmod 6$$

有六个解 $x\equiv 0,\ 1,\ 2,\ 3,\ 4,\ 5 \pmod 6$.

n 次同余方程有 n 个不相同解的条件有下定理：

定理 2 $n(<p)$ 次同余方程 $f(x)\equiv 0 \pmod p$ 有 n 个不相同解的必要充分条件是 $f(x)$ 关于模 p 是 x^p-x 的因式.

证明 设 $x^p-x=q(x)f(x)+r(x)$，这里 $r(x)$ 的次数小于 n. 假如 $f(x)\equiv 0(p)$ 有 n 个解，这 n 个解显然也是 $x^p-x\equiv 0(p)$ 的解，因此也都是 $r(x)\equiv 0(p)$ 的解. 但 $r(x)$ 的次数小于 n. 因此 $r(x)$ 的系数都是 p 的倍数，即 $x^p-x\equiv q(x)f(x) \pmod p$. 反过来，假如 $x^p-x\equiv q(x)f(x) \pmod p$，如果 $f(x)\equiv 0 \pmod p$ 解的个数小于 n，因为 $q(x)\equiv 0(p)$ 的解不能多于 $p-n$ 个，所以 $q(x)f(x)\equiv 0(p)$ 的解小于 p 个，这与上面例2矛盾. 所以 $f(x)\equiv 0$ 的解有 n 个. 定理证毕.

在§2.2中，我们得知 $\varphi(p)=p-1$ 是 p 是质数的必要充分条件，下面威尔生(J. wilson，1741～1793)定理又给出 p 是质数的另一必要充分条件，这是拉格朗日于1770年证得的.

定理 3 整数 p 是质数的必要充分条件是

$$(p-1)!+1\equiv 0 \pmod p. \tag{2}$$

证明 假定 p 是质数，因为 $x\equiv 1,2,\cdots, p-1 \pmod p$ 是 $x^{p-1}-1\equiv 0 \pmod p$ 的解，所以

$$x^{p-1}-1\equiv (x-1)(x-2)\cdots(x-p+1) \pmod p.$$

令 $x=0$，得

$$-1\equiv(-1)^{p-1}(p-1)! \pmod p.$$

当 p 是奇质数时，$p-1$ 是偶数，因此(2) 式成立，当 $p=2$ 时，(2)显然成立，于是必要条件成立.

反过来，假如(2)成立，如果 p 不是质数，命 q 是 p 的真约数，因为 $1<q<p$，所以 $(p-1)!\equiv 0 \pmod q$，于是 $(p-1)!+1\not\equiv 0 \pmod q$，这与(2)矛盾. 所以 p 是质数，因此充分条件成立，定理得证.

譬如 $6!+1=721\equiv 0 \pmod 7$.

用这定理来判别数 n 是否是质数，非常困难，因为就是 n 是 3 位数时，$(n-1)!+1$ 也是超过 100 位的数，计算量很大.

假如 $x_1, \cdots, x_{\varphi(p)}$ 是质数 p 的简化剩余系，由上定理，显然

$$x_1\cdots x_{\varphi(p)}+1\equiv 0 \pmod p,$$

这是(2)的一般形式. 要注意的是这里 p 是质数，如果 p 不是质数，上式不一定成立. 譬如

$$x_1 x_{\varphi(4)}+1\equiv 0 \pmod 4,$$

$$x_1\cdots x_{\varphi(15)}-1\equiv 0 \pmod{15}$$

在 § 5.1 中将另有详细说明.

例 3 假定 p 是质数，n 是正整数，$p\geqslant n>0$，试证

$$(n-1)!\,(p-n)!\equiv(-1)^n \pmod p$$

证 因为$(-1)k\equiv p-k \pmod p$，于是

$$(n-1)!\equiv(-1)^{n-1}(p-1)\cdots(p-n+1) \pmod p$$

因此 $(n-1)!\,(p-n)!\equiv(-1)^{n-1}(p-1)!\equiv(-1)^{n-1}(-1)$
$$\equiv(-1)^n \pmod p$$

特别，当$n=1$时，就是威尔生定理．因此上例可以说是威尔生定理的推广．

习 题 4．2

解下列各方程

1．$3x^{14}+4x^{13}+3x^{12}+2x^{11}+x^9+2x^8+4x^7+x^5+3x^4+x^3+4x^2+2x\equiv0 \pmod 5$．

2．$2x^{17}+6x^{16}+x^{14}+5x^{12}+3x^{11}+2x^{10}+x^9+5x^8+2x^7+3x^5+4x^4+6x^3+4x^2+x+4\equiv0 \pmod 7$．

3．$x^{12}\equiv37 \pmod{41}$．

4．假定p是质数，$n\mid(p-1)$，那末$x^n\equiv1 \pmod p$有n个解．

5．试证$f(x)\equiv0 \pmod p$有p个不相同解的必要充分条件是关于$\bmod p$，x^p-x是$f(x)$的因式．

§4.3 合数模的高次同余方程

同余方程

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\equiv0 \pmod m \quad m\nmid a_0, \tag{1}$$

的解法，基本原则仍然与上节解质数模的一样，先对$f(x)$的系数、次数及模m进行简化，然后以完全剩余系中数代入，

求得其解.

同上节一样，我们可以对 $f(x)$ 进行如下简化：

假如 $(a_n, m)=1$，那末(1)的解都与 m 互质. 如果这时 $f(x)$ 的次数 $\geqq\varphi(m)$，我们可以用 $x^{\varphi(m)}-1$ 除 $f(x)$ 或用 $x^{\varphi(m)}\equiv 1 \pmod m$ 把 $f(x)$ 的次数降低，使问题简化.

下面我们对模 m 简化. 首先假定 $m=m_1m_2$，$(m_1, m_2)=1$，显然(1)与同余方程组

$$\begin{cases} f(x)\equiv 0 \pmod{m_1} \\ f(x)\equiv 0 \pmod{m_2} \end{cases} \tag{2}$$

等价，这就是说(1)的解是(2)的解，反过来(2)的解也是(1)的解，因此求解(1)就变为求解(2)了.

我们这样来求解(2)，先解 $f(x)\equiv 0 \pmod{m_1}$ 及 $f(x)\equiv 0 \pmod{m_2}$ 分别得 $x\equiv a_i \pmod{m_1}$，$i=1, \cdots, r$；$x\equiv b_j \pmod{m_2}$，$j=1, \cdots, s$，显然(2)与 rs 个同余方程组

$$\begin{cases} x\equiv a_i \pmod{m_1} \\ x\equiv b_j \pmod{m_2} \end{cases}, \tag{3}$$

$$i=1, \cdots, r;\ j=1, \cdots, s$$

等价，于是(3)的所有解就是(1)的全部解. 由孙子定理，对于模 m，(3)中任一方程组都有唯一解，因此共 rs 个解，这 rs 个解就是(1)的全部解.

由上面的讨论我们又得知(1)的解的个数等于 $f(x)\equiv 0 \pmod{m_1}$ 的解的个数与 $f(x)\equiv 0 \pmod{m_2}$ 的解的个数的乘积.

例 1 解 $x^4+3x^3+3x^2+3x+2\equiv 0 \pmod{30}$

解 因为 $x^4+3x^3+3x^2+3x+2\equiv 0 \pmod 5$

的解为 $x\equiv -2, -1, 2 \pmod 5$，

$$x^4+3x^3+3x^2+3x+2\equiv 0 \pmod 6$$

的解为 $x\equiv -2,\ -1,\ 1,\ 2 \pmod 6$，

于是同余方程组

$$\begin{cases} x\equiv a_i \pmod 5 \\ x\equiv b_j \pmod 6 \end{cases}$$

的解 $x=6a_i+25b_j \pmod{30}$，

这里 $a_i=-2,\ 1,\ 2$；$b_j=-2,\ -1,\ 1,\ 2$

就是所求解，因此所求解共计 $3\times 4=12$ 个.

$$x\equiv -13,\ -11,\ -8,\ -7,\ -2,\ -1,\ 2,\ 4,\ 7,\ 8,\ 13,\ 14 \pmod{30}$$

下面是 § 4.2 中例 2 的一般形式.

例 2 同余方程

$$x^{\varphi(m)}-1\equiv 0 \pmod m$$

有 $\varphi(m)$ 个解.

证 与 m 不互质的数显然不是所给方程的解，再由 § 2.2 欧拉定理得知任意与 m 互质的数都是它的解，所以它有 $\varphi(m)$ 个解. 证毕.

再为了使模 m 尽可能化小，我们把 m 写成质数幂的乘积，即 $m=p_1^{k_1}\cdots p_r^{k_r}$，于是求解 (1) 归结于求解

$$f(x)\equiv 0 \pmod{p^k} \tag{4}$$

下面我们来讨论（4）的解法，这解法也可以说是解（1）的基本方法.

我们容易知道（4）的解都是

$$f(x)\equiv 0 \pmod p \tag{5}$$

的解，因此我们可以从（5）的解中来求（4）的解. 我们这样

来进行，先从（5）的解中求出

$$f(x)\equiv 0\,(p^2) \tag{6}$$

的解，再从所得的解中求出 $f(x)\equiv 0\,(p^3)$ 的解，这样继续推求，最后得到(4)的解. 假如(5)没有解，当然(4)也就没有解.

假定 $x\equiv x_1 \pmod p$ 是(5)的解，显然 x_1+pt_1，t_1 是任意整数，都是(5)的解，首先我们来挑选 t_1 使 $x\equiv x_1+pt_1 \pmod{p^2}$ 是 (6) 的解. 我们把 $x=x_1+pt_1$ 代入 (6)，得 $f(x_1+pt_1)\equiv 0 \pmod{p^2}$，用台劳公式展开 $f(x_1+pt_1)$ 得

$$f(x_1+pt_1)\equiv f(x_1)+pf'(x_1)t_1\equiv 0 \pmod{p^2}$$

即

$$\frac{f(x_1)}{p}+f'(x_1)t_1\equiv 0 \pmod p. \tag{7}$$

假如 $f'(x_1)\not\equiv 0 \pmod p$，那末上式有唯一个解 $t_1\equiv t'_1 \pmod p$，因此 $x\equiv x_1+pt'_1=x_2 \pmod{p^2}$ 是(6)的解. 同样，因为 $x_1\equiv x_2 \pmod p$，所以 $f'(x_2)\not\equiv 0 \pmod p$，于是由 x_2 我们又可求得 $f(x)\equiv 0\,(p^3)$ 的解 $x_3=x_2+p^2t'_2$. 一般假定我们已求得 $x\equiv x_{k-1} \pmod{p^{k-1}}$ 是 $f(x)\equiv 0 \pmod{p^{k-1}}$ 的解，即 $f(x_{k-1})\equiv 0 \pmod{p^{k-1}}$，我们把 $x=x_{k-1}+p^{k-1}t_{k-1}$ 代入 (4) 得

$$\begin{aligned} &f(x_{k-1}+p^{k-1}t_{k-1})\\ &\quad\equiv f(x_{k-1})+p^{k-1}f'(x_{k-1})t_{k-1}\equiv 0 \pmod{p^k}, \end{aligned}$$

即

$$\frac{f(x_{k-1})}{p^{k-1}}+f'(x_{k-1})t_{k-1}\equiv 0 \pmod p. \tag{8}$$

我们容易知道 $x_{k-1}\equiv x_1 \pmod p$，因此 $f'(x_{k-1})\not\equiv 0 \pmod p$，所以（8）有唯一个解 $t_{k-1}\equiv t'_{k-1} \pmod p$，于是 $x\equiv x_{k-1}+p^{k-1}t'_{k-1}=x_k \pmod{p^k}$ 就是（4）的解，这就是说我们已求得 x_{k-1} 后，再解（8）得 t'_{k-1}，那末 $x_k=x_{k-1}+p^{k-1}t'_{k-1}$ 就是（4）的解.

于是我们得知，假如已知 $x \equiv x_1 \pmod p$ 是(5)的一个解，只要 $f'(x_1) \not\equiv 0 \pmod p$，我们就可以在与 x_1 同余的数中(对于模 p)求得(4)的一个解．

假如 $f'(x_1) \equiv 0 \pmod p$，如果 $\frac{f(x_1)}{p} \not\equiv 0 \pmod p$，那末(7)无解，因此在对于模 p，与 x_1 同余的数中，(4)没有解，如果 $\frac{f(x_1)}{p} \equiv 0 \pmod p$，那末(7)有 p 个解，因此这时(6)也有 p 个解，也就是说这时有 p 个 x_2，对于每个 x_2，显然 $f'(x_2) \equiv 0 \pmod p$．但 $\frac{f(x_2)}{p^2} \equiv 0 \pmod p$ 就不一定成立，因此这时由 $x \equiv x_1 \pmod p$ 能否求得 $f(x) \equiv 0 \pmod{p^3}$ 的解，以及求得若干个解，并无一般结论．求解这类同余式只有按照上述方法具体推导．

由上面讨论我们得知只要 $f(x) \equiv 0 \pmod p$ 与 $f'(x) \equiv 0 \pmod p$ 没有公共解．由(5)的一个解就可求得(4)的一个解，并且由(5)的不相同的解求得的(4)的解也是不相同的．于是我们有：

定理 假如 $f(x) \equiv 0 \pmod p$ 与 $f'(x) \equiv 0 \pmod p$ 没有公共解，那末(4)的解个数与(5)的解的个数相等．

例 3 解 $x^3 - 2x + 6 \equiv 0 \pmod{125}$

解 因为 $f(x) = x^3 - 2x + 6 \equiv 0 \pmod 5$ 即 $x^3 - 2x + 1 \equiv 0 \pmod 5$ 有两个解 $x = 1, 2$．先讨论 $x_1 = 1$，这时 $f(1) = 5$，$f'(1) = 1$，解同余方程

$$\frac{5}{5} + t_1 \equiv 0 \pmod 5$$

即

$$1 + t_1 \equiv 0 \pmod 5$$

得 $t_1\equiv-1\pmod 5$， 因此 $x_2\equiv 1+5t_1=-4\pmod{25}$ 是 $f(x)\equiv 0\pmod{25}$的解．再因为$f(-4)=-50, f'(-4)=46$，解同余方程

$$-2+46t_2\equiv 0\pmod 5$$

即

$$-2+t_2\equiv 0\pmod 5$$

得 $t_2\equiv 2\pmod 5$．于是所求解为

$$x\equiv -4+25.2=46\pmod{125}$$

再讨论 $x_1=2$，这时 $f(2)=10$， $f'(2)=10$， 同余方程

$$2+10t_1\equiv 0\pmod 5$$

显然无解．所以，这时所给同余方程也无解．因此上面求得的 $x\equiv 46\pmod{125}$ 是所求的唯一解．解毕．

例 4 假定$(a, m)=1$，$x\equiv x_0\pmod m$ 是同余方程

$$x^n\equiv a\pmod m, \quad n>0,$$

的一个解，试证这同余方程所有解是 x_0 与同余方程

$$y^n\equiv 1\pmod m$$

的所有解的乘积．

证 显然从 $x_0^n\equiv a\pmod m$，$y^n\equiv 1\pmod m$ 即得 $(x_0y)^n\equiv a\pmod m$．再如果 $y_1\not\equiv y_2\pmod m$，那末 $x_0y_1\not\equiv x_0y_2\pmod m$．又从 $x_0^n\equiv a\pmod m$，$x^n\equiv a\pmod m$ 得 $x^n\equiv x_0^n\pmod m$．因为 $(x_0, m)=1$，假如 $x_0y\equiv x\pmod m$，那末 $(x_0y)^n\equiv x^n\equiv x_0^n\pmod m$，因此$y^n\equiv 1\pmod m$．证毕．

习 题 3.4

解下列各同余方程

1. $x^4+7x+4\equiv 0 \pmod{27}$.

2. $x^2-5x+7\equiv 0 \pmod{9}$.

3. $x^4-8x^3+9x^2+9x+14\equiv 0 \pmod{25}$.

4. $6x^3+27x^2+17x+20\equiv 0 \pmod{30}$.

5. $x^3+x^2-x-1\equiv 0 \pmod{15}$.

6. $4x^3+3x+43\equiv 0 \pmod{125}$.

7. 解同余式方程组

   $x\equiv 3 \pmod{8}$, $x\equiv 11 \pmod{20}$, $x\equiv 1 \pmod{15}$.

第五章　平方剩余与二次同余方程

从上章我们得知，求解一般二次同余方程可以归结于求解质数模的二次同余方程．一般质数模的二次同余方程可以写成

$$x^2 \equiv a \pmod{p} \tag{1}$$

当(1)有解时，那末 a 就是某平方数用 p 来除的剩余，因此我们叫 a 是 p 的**平方剩余**，否则也就是(1)没有解时，我们叫 a 是 p 的平方非剩余．

这章我们讨论二个问题．第一个问题讨论平方剩余，也就是讨论对已知的质数 p，哪些 a 是它的平方剩余，哪些 a 是它的平方非剩余；又对已知 a，关于哪些质数 p，它是平方剩余，关于哪些质数 p，它是平方非剩余．第二个问题是求解(1)，上章虽然是讨论了解一般同余方程，但没有具体讨论解二次同余方程，这里也可以说是它的补充．

§5.1　基本性质

质数 p 模的二次同余方程是

$$ax^2+bx+c\equiv 0 \pmod{p}, \quad p\nmid a$$

当 $p=2$ 时，它的解当然很容易求出，因此我们假定 p 是奇质数．因为 $(a, p)=1$，所以有使 $aa'\equiv 1 \pmod{p}$ 成立的整数 a'，用 a' 乘两边，得

$$x^2+a'bx+a'c\equiv o\pmod p,$$

假如 $a'b$ 不是偶数，我们可以把它改成偶数 $a'b+p=2b_1$，因此我们有

$$x^2+2b_1x+c_1\equiv o\pmod p,$$

即
$$(x+b_1)^2\equiv b_1^2-c_1\pmod p,$$

这就是说质数 p 模的一般二次同余方程可以化为（1）的形式，因为 $a\equiv 0\pmod p$ 时，（1）的解是 $x\equiv 0\pmod p$，情况非常简单，所以我们还假定 $p\nmid a$.

要注意的是对于质数模 p 的二次同余方程才能化成（1）这样简单形状，对一般合数模的二次同余方程不一定能如此.

假如 $x\equiv\alpha\pmod p$ 是（1）的解，显然 $x\equiv-\alpha\pmod p$ 也是（1）的解. 因为 p 是奇质数，并且 $p\nmid a$，所以 $\alpha\not\equiv-\alpha\pmod p$，这就是说 $x\equiv\pm\alpha\pmod p$ 是（1）的二个不相同的解. 于是我们得知，假如（1）有解，那末它就有二个不相同的解.

下面我们来讨论第一个问题.

假如 p 是奇质数，

$$x^2\equiv a\pmod p,\quad p\nmid a \tag{1}$$

有解，那末它的解必定是与 p 的简化剩余系 $\pm1,\ \pm2,\cdots,\ \pm\frac{1}{2}(p-1)$ 中数同余，因此与

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{1}{2}(p-1)\right)^2$$

中一数同余的数都是 p 的平方剩余，显然在 p 的简化剩余系中除与这些数同余的外，其他都是 p 的平方非剩余. 再这

$\frac{1}{2}(p-1)$个数关于模 p 又两两互不同余，这是因为如果

$$i^2 \equiv j^2 \pmod p,\ 1 \leq j < i \leq \frac{1}{2}(p-1),$$

那末 $$(i-j)(i+j) \equiv 0 \pmod p.$$

因此 $p \mid (i-j)$ 或 $p \mid (i+j)$，这都与假设不合，于是我们有：

定理 1 在奇质数 p 的简化剩余系中，$\frac{1}{2}(p-1)$ 个数是 p 的平方剩余，它们分别与

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{1}{2}(p-1)\right)^2$$

同余，其他$\frac{1}{2}(p-1)$个数是 p 的平方非剩余.

譬如 $p=17$ 时，$\frac{1}{2}(p-1)=8$，因为

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 16,$$
$$5^2 \equiv 8,\ 6^2 \equiv 2,\ 7^2 \equiv 15,\ 8^2 \equiv 13,$$

所以 $$1,\ 2,\ 4,\ 8,\ 9,\ 13,\ 15,\ 16$$

8 个数是 17 的平方剩余，其他

$$3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14,$$

8 个数是 17 的平方非剩余.

上面的定理解答了第一个问题的第一部分，下面我们来讨论第二部分，但这部分的讨论非常困难，远不如上面简单，它是平方剩余的主要内容.

假如 a 是 p 的平方剩余，即（1）有解，因此我们有 $x^2 \equiv a \pmod p$，于是 $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$，但由费马定理

$a^{p-1}\equiv 1 \pmod p$，所以 $a^{\frac{p-1}{2}}\equiv 1 \pmod p$．反过来，假如 $a^{\frac{p-1}{2}}\equiv 1 \pmod p$，那末 a 是同余方程 $x^{\frac{p-1}{2}}\equiv 1 \pmod p$ 的解，因为它的解的个数不大于 $\frac{1}{2}(p-1)$，所以

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{1}{2}(p-1)\right)^2$$

就是它的全部解，因此 a 必与其中某 i^2 同余，即

$$a\equiv i^2 \pmod p.$$

于是（1）有解，所以 a 是 p 的平方剩余．

再假如 a 是 p 的平方非剩余，即（1）无解，由费马定理，我们有

$$a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)\equiv 0 \pmod p.$$

因为 $a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$，所以 $a^{\frac{p-1}{2}}\equiv -1 \pmod p$．反过来假如 $a^{\frac{p-1}{2}}\equiv -1 \pmod p$，那末 $a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$，因为不如此我们就有 $2\equiv 0 \pmod p$，这显然是矛盾．所以（1）无解．因此，a 是 p 的平方非剩余．

于是我们有下面著名的欧拉判别法．

定理 2 假定 p 是奇质数，$p\nmid a$，那末 a 是 p 的平方剩余的必要充分条件是

$$a^{\frac{p-1}{2}}\equiv 1 \pmod p;$$

a 是 p 的平方非剩余的必要充分条件是

$$a^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

譬如$(-1)^{\frac{1}{2}(5-1)}=(-1)^2\equiv 1 \pmod 5$，$3^{\frac{1}{2}(5-1)}=9\equiv -1 \pmod 5$，所以$-1$是5的平方剩余，3是5的平方非剩余，即$x^2\equiv -1 \pmod 5$有解，$x^2\equiv 3 \pmod 5$无解。

由上面定理2我们容易推得：

定理 3 假定a，b是与奇质数p互质的两个整数，

(1) 当a，b都是p的平方剩余或都是平方非剩余时，那末ab是p的平方剩余。

(2) 当a，b中有一是p的平方剩余，另一是p的平方非剩余时，那末ab是p的平方非剩余。

上面是平方剩余的基本性质，至于第二部分的解答，在下节我们将以简单的符号给出。

§5.2 勒朗德符号

平方剩余的性质用下面勒朗德符号$\left(\frac{a}{p}\right)$表示极为方便，因此下面的讨论我们就从勒朗德符号开始。

定义 假定p是奇质数，$(a, p)=1$，我们规定

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{当 } a \text{ 是 } p \text{ 的平方剩余；}\\ -1, & \text{当 } a \text{ 是 } p \text{ 的平方非剩余。}\end{cases}$$

这就是说勒朗德符号$\left(\frac{a}{p}\right)$是表示$+1$或-1，当a是p的平方剩余时，$\left(\frac{a}{p}\right)=+1$，当$a$是$p$的平方非剩余时，$\left(\frac{a}{p}\right)=-1$。

譬如　$\left(\frac{1}{17}\right)=+1$，$\left(\frac{3}{17}\right)=-1$，

由定义我们容易得知

$$\left(\frac{1}{p}\right)=1,\quad \left(\frac{a^2}{p}\right)=1,$$

并且当 $a\equiv b \pmod p$ 时，

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

根据上节定理 2 我们有

定理 1　假定 p 是奇质数，$(a, p)=1$，那末

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p.$$

再我们有

定理 2　$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$

证明　因为

$$\left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}}$$

$$\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p,$$

而$\left(\frac{a}{p}\right)$，$\left(\frac{b}{p}\right)$，$\left(\frac{ab}{p}\right)$不是 $+1$，便是 -1．又 p 是奇质数，因此定理得证．

譬如$\left(\frac{12}{17}\right)=\left(\frac{3}{17}\right)\left(\frac{2^2}{17}\right)=\left(\frac{3}{17}\right)=-1$，

即同余方程 $x^2\equiv 12 \pmod{17}$ 无解．

一般我们不难推得

$$\left(\frac{a_1a_2\cdots a_k}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_k}{p}\right).$$

有了上面的性质，就比较容易讨论我们提出的问题了.

假如 $a=\pm 2^{a_0}q_1^{a_1}\cdots q_k^{a_k}$，那末

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{a_0}\left(\frac{q_1}{p}\right)^{a_1}\cdots\left(\frac{q_k}{p}\right)^{a_k}$$

因此，判别$\left(\frac{a}{p}\right)$的问题就归结于判别

$$\left(\frac{\pm 1}{p}\right),\ \left(\frac{2}{p}\right),\ \left(\frac{q}{p}\right),\ p,\ q\text{ 都是奇质数}$$

的问题，下面我们来分别讨论.

定理 3 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

证明 由定理 1，我们有

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p$$

但$\left(\frac{-1}{p}\right)$，$(-1)^{\frac{p-1}{2}}$是 $+1$ 或 -1，而 p 又是奇质数，所以定理成立.

于是当$\frac{1}{2}(p-1)\equiv 0\pmod 2$，即 $p\equiv 1\pmod 4$时，$\left(\frac{-1}{p}\right)=1$；当$\frac{1}{2}(p-1)\equiv -1\pmod 2$，即 $p\equiv -1\pmod 4$时，$\left(\frac{-1}{p}\right)=-1$，也就是说当 $p=4n+1$ 时，

$$\left(\frac{-1}{p}\right)=1;$$

当 $p=4n-1$ 时，

$$\left(\frac{-1}{p}\right)=-1.$$

譬如 $p=5$，13，17，29，…，时，$\left(\frac{-1}{p}\right)=1$；$p=3$，

7，11，19，23，…，时，$\left(\frac{-1}{p}\right)=-1$.

为了讨论$\left(\frac{2}{p}\right)$，我们需要下面的高斯引理.

定理 4 $\left(\frac{a}{p}\right)=(-1)^{\mu}$，

这里$\mu(\geqslant 0)$是

$$a,\ 2a,\ \cdots,\ \frac{1}{2}(p-1)a \tag{1}$$

中各数用p除得到的最小正剩余中大于$\frac{p}{2}$的个数.

譬如$a=3$，$p=11$时，$\frac{p-1}{2}=5$，用11除下列各数

$$3,\ 6,\ 9,\ 12,\ 15$$

得到的最小正剩余分别为

$$3,\ 6,\ 9,\ 1,\ 4$$

其中大于5的只有6，9二数，因此$\mu=2$，于是$\left(\frac{3}{11}\right)=(-1)^2=1$，即$x^2\equiv 3\pmod{11}$有解，显然$5^2-3=22\equiv 0\pmod{11}$，所以$x\equiv\pm 5\pmod{11}$就是它的解.

现在我们来证明高斯引理.

因为在p的简化剩余系$1,2,\cdots p-1$中小于$\frac{p}{2}$的数是$1,\ 2,\ \cdots,\ \frac{p-1}{2}$，大于$\frac{p}{2}$的数是$\frac{p+1}{2}$，…，$p-2$，$p-1$. 又因为(1)是$p$的简化剩余系的一部分，所以(1)中用$p$除得到的剩余如果小于$\frac{p}{2}$，它就与$1,\ 2,\cdots,\frac{p-1}{2}$中一数关于$p$同余，如果大于$\frac{p}{2}$，它就与$\frac{p+1}{2}$，…，$p-2$，

$p-1$ 中一数也就是与 $-\frac{p-1}{2}$, …, -2, -1 中一数关于 p 同余. 再在(1)中, 那 μ 个数中一数与其他 $\frac{p-1}{2}-\mu$ 个数中一数不能与只是符号相反的数同余, 这是因为如果 $ka\equiv b \pmod p$, $la\equiv -b \pmod p$, 那末 $(k+l)a\equiv 0 \pmod p$, 因为 $(a,p)=1$, $2\leqslant k+l<p$, 这显然是矛盾. 于是我们有

$$a,\ 2a\cdots\frac{1}{2}(p-1)a\equiv(-1)^{\mu}\,1.2\cdots\frac{p-1}{2} \pmod p.$$

但 $1.2\cdots\frac{p-1}{2}$ 与 p 互质, 所以

$$a^{\frac{p-1}{2}}\equiv(-1)^{\mu} \pmod p,$$

即
$$\left(\frac{a}{p}\right)\equiv(-1)^{\mu} \pmod p.$$

因为 $p>2$, 而上式两边不外是 $+1$ 或 -1, 所以

$$\left(\frac{a}{p}\right)=(-1)^{\mu}.$$

于是定理成立.

上定理中的 μ 还可以用具体的式子来表达.

定理 5 $\mu\equiv\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ka}{p}\right]+\frac{p^2-1}{8}(a-1) \pmod 2.$

证明 命
$$ka=\left[\frac{ka}{p}\right]p+r_k,$$

$$1\leqq k\leqq\frac{1}{2}(p-1),\quad 1\leqq r_k\leqq p-1,$$

于是
$$\sum_{k=1}^{\frac{1}{2}(p-1)}ka=\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ka}{p}\right]p+\sum_{k=1}^{\frac{1}{2}(p-1)}r_k,$$

再假设$r_1, \cdots, r_\mu$都大于$\frac{p}{2}$，那末$r_{\mu+1}, \cdots, r_{\frac{p-1}{2}}$都小于$\frac{p}{2}$，因此$p-r_1$，$\cdots$，$p-r_\mu$，$r_{\mu+1}$，$\cdots$，$r_{\frac{p-1}{2}}$与1，2，$\cdots$，$\frac{p-1}{2}$一致，所以

$$\sum_{k=1}^{\frac{1}{2}(p-1)} k = \mu p - (r_1 + \cdots + r_\mu) + (r_{\mu+1} + \cdots + r_{\frac{p-1}{2}}),$$

即
$$r_{\mu-1} + \cdots + r_{\frac{p-1}{2}} = \sum_{k=1}^{\frac{1}{2}(p-1)} k - \mu p + (r_1 + \cdots + r_\mu)$$

于是
$$\sum_{k=1}^{\frac{1}{2}(p-1)} ka = \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p}\right] p + \sum_{k=1}^{\frac{1}{2}(p-1)} k - \mu p - 2(r_1 + \cdots + r_\mu)$$

因为$p \equiv 1 \pmod 2$，所以

$$\mu \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p}\right] - \sum_{k=1}^{\frac{1}{2}(p-1)} k(a-1) \pmod 2$$

但
$$\sum_{k=1}^{\frac{1}{2}(p-1)} k = \frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} = \frac{p^2-1}{8},$$

于是
$$\mu \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p}\right] - \frac{p^2-1}{8}(a-1)$$

$$\equiv \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p}\right] + \frac{p^2-1}{8}(a-1) \pmod 2,$$

因此定理得证.

特别，当 a 是奇数时，$a-1$ 是偶数，因此这时

$$\mu \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p}\right] \pmod 2.$$

譬如 $a=3$，$p=11$ 时，$\frac{1}{2}(p-1)=5$，所以

$$\mu=\sum_{k=1}^{5}\left[\frac{3k}{11}\right]=\left[\frac{3}{11}\right]+\left[\frac{6}{11}\right]+\left[\frac{9}{11}\right]+\left[\frac{12}{11}\right]+\left[\frac{15}{11}\right]$$

$$=0+0+0+1+1=2,$$

这结果与前面算得的一致.

现在我们来讨论$\left(\frac{2}{p}\right)$.

定理 6 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

证明 因为在上定理中，$1 \leqslant k \leqslant \frac{1}{2}(p-1)$，所以

$$2 \leqq 2k \leqq p-1,$$

这时 $a=2$，因此

$$\left[\frac{2k}{p}\right]=0, \text{ 即 } \sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{ka}{p}\right]=0,$$

于是由上定理得

$$\mu \equiv \frac{p^2-1}{8} \pmod 2,$$

所以定理成立.

当$\frac{p^2-1}{8} \equiv 0 \pmod 2$时，我们有

$$\frac{p-1}{2}\cdot\frac{p+1}{2}\equiv 0 \pmod 4,$$

但
$$\frac{p-1}{2}+\frac{p+1}{2}=p,$$

因此$\frac{1}{2}(p-1)$，$\frac{1}{2}(p+1)$中必有一是奇数，一是偶数，于是

$$\frac{p-1}{2}\equiv 0 \text{ 或 } \frac{p+1}{2}\equiv 0 \pmod 4$$

即
$$p\equiv 1 \text{ 或 } p\equiv -1 \pmod 8$$

这就是说只有当$p\equiv \pm 1 \pmod 8$时，2是它们的平方剩余。

当$\frac{p^2-1}{8}\equiv 1 \pmod 2$时，我们有

$$\frac{p-3}{2}\cdot\frac{p+3}{2}\equiv 0 \pmod 4$$

同上面一样，我们得$p\equiv 3$，或$p\equiv -3 \pmod 8$，这就是说只有当$p\equiv \pm 3 \pmod 8$时，2是它们的平方非剩余。

于是我们得知当$p=8n\pm 1$时，

$$\left(\frac{2}{p}\right)=+1;$$

当$p=8n\pm 3$时，

$$\left(\frac{2}{p}\right)=-1.$$

譬如$p=7$，17，23，31，41时，$\left(\frac{2}{p}\right)=+1$；$p=3$，5，11，13，19时，$\left(\frac{2}{p}\right)=-1$。

现在只剩下$\left(\frac{a}{p}\right)$没有讨论，这问题不象上面那样简单能给出一般的结论，但是引用下面著名的高斯互反律，我们可

以把对已知 q，讨论 $\left(\frac{q}{p}\right)$的问题变成讨论$\left(\frac{p}{q}\right)$的问题，这样问题就简化多了.

下面是著名的高斯互反律，这结果是 1783 年欧拉首先发现的，1785 年勒朗德又重新提出，但他们都没有证明，直到 1796 年高斯才给出严格证明.

定理 7 假定 p，q 是两个不同的奇质数，那末，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

即

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

证明 因为$\left(\frac{q}{p}\right)=(-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]}$，

$$\left(\frac{p}{q}\right)=(-1)^{\sum\limits_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]},$$

所以

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\sum\limits_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum\limits_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]},$$

下面我们这样来证明下式：

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2} \quad (3)$$

取$\frac{p-1}{2}\cdot\frac{q-1}{2}$个数

$$lp-kq,$$

这里$l=1, 2, \cdots, \frac{1}{2}(q-1)$；$k=1, 2, \cdots, \frac{1}{2}(p-1)$，其中显然无一为零，这是因为如果$lp=kq$，那末$q\mid lp$，这与$(p, q)=1$，$l<q$矛盾，再在这$\frac{p-1}{2}\cdot\frac{q-1}{2}$个数中，假如我们能够证明正数有$\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]$个，负数有$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]$个，那末(3)式就显然成立.

我们知道对于给出的l，$lp-kq>0$的必要充分条件是$\frac{lp}{q}>k$，即 $1\leqq k\leqq\left[\frac{lp}{q}\right]$，但

$$\frac{lp}{q}<\frac{\frac{q}{2}p}{q}=\frac{1}{2}p,$$

所以
$$\left[\frac{lp}{q}\right]\leqq\frac{1}{2}(p-1),$$

因此当l给定时，这样的k就有$\left[\frac{lp}{q}\right]$个，于是在$lp-kq$中，正数有$\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]$个. 同样，负数有$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]$个，所以(3)成立，因此定理得证.

于是假如p, q中有一是$4n+1$形状，那末$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=1$，即 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$，如果$p, q$都是$4n-1$形状，

那末
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=-1,$$
即
$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right).$$

到此，我们的第一个问题完全解决了.

例 1 求$\left(\frac{219}{383}\right)$，383是质数.

解
$$\left(\frac{219}{383}\right)=\left(\frac{3}{383}\right)\left(\frac{73}{383}\right),$$
但
$$\left(\frac{3}{383}\right)=(-1)^{\frac{383-1}{2}\cdot\frac{3-1}{2}}\left(\frac{383}{3}\right)$$
$$=-\left(\frac{383}{3}\right)=-\left(\frac{2}{3}\right)=+1,$$
$$\left(\frac{73}{383}\right)=(-1)^{\frac{383-1}{2}\cdot\frac{73-1}{2}}\left(\frac{383}{73}\right)=\left(\frac{383}{73}\right)$$
$$=\left(\frac{18}{73}\right)=\left(\frac{3^2}{73}\right)\left(\frac{2}{73}\right)=\left(\frac{2}{73}\right)=+1.$$
所以$\left(\frac{219}{383}\right)=+1$，即219是383的平方剩余.

例 2 求以3为平方剩余或平方非剩余的奇质数p.

解 由互反律
$$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right),$$
因此$(-1)^{\frac{p-1}{2}}$，$\left(\frac{p}{3}\right)$当他们同为1或同为-1时，$\left(\frac{3}{p}\right)=+1$，一为1，一为$-1$时，$\left(\frac{3}{p}\right)=-1$.

显然，当 $\frac{p-1}{2}$ 是偶数，即 $p\equiv1\pmod 4$ 时，$(-1)^{\frac{p-1}{2}}=+1$，当 $\frac{p-1}{2}$ 是奇数，即 $p\equiv-1\pmod 4$ 时，$(-1)^{\frac{p-1}{2}}=-1$.

再因为 p 是奇质数，关于模 3 我们有 $p\equiv1$ 或 $p\equiv-1$，当 $p\equiv1\pmod 3$ 时，$\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$，当 $p\equiv-1\pmod 3$ 时，$\left(\frac{p}{3}\right)=\left(\frac{-1}{3}\right)=-1$.

于是所求的 p 是下列一同余方程组的解

$$\begin{cases}p\equiv1\pmod 3\\p\equiv1\pmod 4,\end{cases}\qquad\begin{cases}p\equiv-1\pmod 3\\p\equiv-1\pmod 4,\end{cases}$$

$$\begin{cases}p\equiv1\pmod 3\\p\equiv-1\pmod 4,\end{cases}\qquad\begin{cases}p\equiv-1\pmod 3,\\p\equiv1\pmod 4.\end{cases}$$

即 $p\equiv1$，$p\equiv-1$，$p\equiv-5$，$p\equiv5\pmod{12}$，因此当 $p\equiv\pm1\pmod{12}$ 时，$\left(\frac{3}{p}\right)=+1$，当 $p\equiv\pm5\pmod{12}$ 时，$\left(\frac{3}{p}\right)=-1$，也就是说当 $p=12n\pm1$ 时，3 是平方剩余，当 $p=12n\pm5$ 时，3 是平方非剩余．解毕．

下面是 §2·2 定理 10 的另一证明①

例 3 试证费马数 $F_n=2^{2^n}+1$ $(n>1)$ 的质因数是 $2^{n+2}t+1$ 形状．

证 由 §2·2 定理 9 得知 F_n 的质因数 p 是 $2^{n+1}t+1$ 形状，因此 $p=8h+1$，于是 2 是 p 的平方剩余，即 $2^{\frac{p-1}{2}}\equiv$

① 这证明是洪伯阳给出的．

$1 \pmod p$. 但 $p \mid F_n$, 所以 $2^{2^n} \equiv -1 \pmod p$, 因此 $2^{2^{n+1}} \equiv 1 \pmod p$. 显然 2^{n+1} 是满足 $2^x \equiv 1 \pmod p$ 的最正整数，所以 $2^{n+1} \left| \frac{p-1}{2} \right.$, 即 $p = 2^{n+2}t + 1$. 证毕.

威尔生定理高斯曾把它推广，下面就是这著名的推广定理

例 4 假定 a_1, …, $a_{\varphi(m)}$ 是 m 的简化剩余系，那末当 $m = 4$, p^n, $2p^n$, 这里 p 是奇质数时，

$$a_1 \cdots a_{\varphi(m)} + 1 \equiv 0 \pmod m,$$

当 m 是其他数时，

$$a_1 \cdots a_{\varphi(m)} - 1 \equiv 0 \pmod m.$$

证 1. 设 $m = p^n$, 设 b 是 p 的平方非剩余，因为 $a_i x \equiv b \pmod{p^n}$ 有唯一解，此解显然是某 a_j, 并且 $a_j \neq a_i$, 否则 $a_i^2 \equiv b \pmod p$, 这与 b 是 p 的平方非剩余的假设不合. 如果我们把这样的 a_i, a_j 作为一对，那末所有 a_1, …, $a_{\varphi(p^n)}$ 可以分为 $\frac{1}{2}\varphi(p^n)$ 个对，于是

$$a_1 \cdots a_{\varphi(p^n)} \equiv b^{\frac{1}{2}\varphi(p^n)} \pmod{p^n}.$$

但 b 是 p 的平方非剩余，所以 $b^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, 因此

$$\left(b^{\frac{1}{2}(p-1)}\right)^{p^{n-1}} = (-1 + kp)^{p^{n-1}}$$

即 $$b^{\frac{1}{2}p^{n-1}(p-1)} = -1 + rp^n,$$

于是 $$b^{\frac{1}{2}\varphi(p^n)} \equiv -1 \pmod{p^n},$$

所以 $$a_1 \cdots a_{\varphi(p^n)} \equiv -1 \pmod{p^n}.$$

2. 设 $m=2p^n$，c 是同余方程组

$$\begin{cases}x\equiv b(\bmod p)\\ x\equiv 1(\bmod 2)\end{cases}$$

的解，那末 $x^2\equiv c(\bmod 2p^n)$ 无解，或者说 c 是 $2p^n$ 的平方非剩余，这是因为如果它有解，那末 $b\equiv c(\bmod p)$ 是 p 的平方剩余．这与假设不合．于是同上面一样，把 $a_ix\equiv c(\bmod 2p^n)$ 的解 a_j 与 a_i 作为一对，我们就得到

$$a_1\cdots a_{\varphi(2p^n)}\equiv c^{\frac{1}{2}\varphi(2p^n)}(\bmod 2p^n)$$

但 $c^{\frac{1}{2}\varphi(p^n)}\equiv -1(\bmod p^n)$，$c$ 是奇数，$\varphi(2p^n)=\varphi(p^n)$，所以

$$c^{\frac{1}{2}\varphi(2p^n)}\equiv -1(\bmod 2p^n)$$

因此 $$a_1\cdots a_{\varphi(2p^n)}\equiv -1(\bmod 2p^n)$$

3. 设 $m=2^n$，$n>2$，因为 -1 是 2^n 的平方非剩余，所以 $a_ix\equiv -1(\bmod 2^n)$ 的解 a_j 与 a_i 作为一对把 $a_1,\cdots,a_{2^{n-1}}$ 分为 2^{n-2} 个对，于是

$$a_1\cdots a_{2^{n-1}}\equiv(-1)^{2^{n-2}}\equiv 1(\bmod 2^n).$$

4. 设 $m=2^{n_0}p_1^{n_1}\cdots p_r^{n_r}$，$p_i$ 是奇质数，b 是 p_1 的平方非剩余，c 是同余方程组

$$\begin{cases}x\equiv b(\bmod p_1)\\ x\equiv 1(\bmod 2p_2\cdots p_r)\end{cases}$$

的解．那末 c 是 m 的平方非剩余．于是根据 $a_ix\equiv c(\bmod m)$ 的解，得

$$a_1\cdots a_{\varphi(m)}\equiv c^{\frac{1}{2}\varphi(m)}\quad(\bmod m)$$

因为 $c^{\frac{1}{2}(p_1-1)}\equiv -1\ (\bmod p_1)$，所以 $c^{\frac{1}{2}\varphi(p_1^{n_1})}\equiv -1(\bmod p^{n_1})$.

但 $\varphi(m)=\varphi(p_1^{n_1})\cdots\varphi(p_r^{n_r})$，而 $\varphi(p_i^{n_i})$ 是偶数，因此

$$c^{\frac{1}{2}\varphi(m)} \equiv +1 \pmod{p_1^{n_1}}$$

再因为 $c=1+2p_2\cdots p_rk$，所以

$$c^{\frac{1}{2}\varphi(m)} = (1+2p_2\cdots p_rk)^{\frac{1}{2}\varphi(m)},$$

因此
$$c^{\frac{1}{2}\varphi(m)} \equiv +1 \pmod{p_2^{n_2}\cdots p_r^{n_r}}$$

又因为 $c^{2^{n_0-1}}\equiv +1 \pmod{2^{n_0}}$，所以 $c^{\frac{1}{2}\varphi(m)} \equiv +1 \pmod{2^{n_0}}$.
于是

$c^{\frac{1}{2}\varphi(m)} \equiv +1 \pmod{m}$. 即 $a_1\cdots a_{\varphi(m)}\equiv +1 \pmod{m}$.
$m=4$ 时定理显然成立，例证毕.

习　题　5.2

1. 计算

$\left(\frac{88}{109}\right)$，$\left(\frac{365}{1847}\right)$，$\left(\frac{-1457}{2389}\right)$，1847，2389 都是质数.

2. 求证不定方程 $x^2+23y=17$ 无解.
3. 求 23 的平方剩余及平方非剩余.
4. 求以 7 为平方非剩余的奇质数.
5. 设 p，q 是奇质数，$p=q+4a$ 求证.

   1) $\left(\frac{p}{q}\right)=\left(\frac{a}{q}\right)$，

   2) $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$.

6. 试证同余方程 $x^2+1\equiv 0 \pmod p$ 有解的必要充分条件是奇质数 p 是 $4k+1$ 的形状，并利用威尔生定理证明它的解是 $x\equiv\pm 1\cdot 2\cdot\cdots\cdot(2k) \pmod p$.

7. 假如 $(x,\ 3)=1$，试证 x^2+3 的奇质因数 p 一定是 $6k+1$ 的形状.

8. 假如 $(x,\ y)=1$，试求 x^2+y^2 及 x^2-2y^2 的奇质因数的形状.

9. 证明形状是 $4k+1$ 及 $6k+1$ 的质数都有无穷多个.

§5.3 亚可比符号

我们的第一个问题在上节用勒朗德符号已完全解决，而且还解决得非常好，美中不足的，只是在计算勒朗德符号时还稍嫌麻烦，原因在勒朗德符号 $\left(\frac{a}{p}\right)$ 中分母 p 要求是奇质数，因此在需要用互反律时，就必须先判别分子是否是质数，假如是合数还要把分子化为质数的乘积，然后才能引用. 这样在计算上造成了很多困难，为了克服这些困难，简化计算，这节我们介绍比勒朗德符号更广泛的亚可比(C. G. J. Jacobi, 1804～1851)符号.

定义 假定 P 是奇数，$P=p_1p_2\cdots p_m$ 是它的质因数分解(当 $i\neq j$ 时可能 $p_i=p_j$)，并且 $(a,\ P)=1$，我们规定

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right),$$

其中右边的 $\left(\frac{a}{p_i}\right)$ 是勒朗德符号，我们把左边的 $\left(\frac{a}{P}\right)$ 叫做亚可比符号. 当 P 是质数时，亚可比符号就是勒朗德符号，

因此亚可比符号是勒朗德符号的推广.

亚可比符号$(\frac{a}{P})$也与勒朗德符号一样是表示$+1$或-1. 当$(\frac{a}{P})=-1$时，同余方程

$$x^2\equiv a \pmod P \tag{1}$$

无解，这是因为假如(1)有解，显然$x^2\equiv a \pmod{p_i}$都有解. 因此$(\frac{a}{p_i})=1$，这与$(\frac{a}{P})=-1$的假设不合，但当$(\frac{a}{P})=+1$时，(1)不一定有解，因为这时可能有偶数个$(\frac{a}{p_i})=-1$，于是$x^2\equiv a \pmod{p_i}$无解，当然(1)也无解，这是与勒朗德符号不同之处.

下面我们来讨论亚可比符号的性质，这些性质在形式上大都与勒朗德符号的类似. 引用这些性质，我们可以把勒朗德符号作为亚可比符号来计算，因而简化了计算勒朗德符号的过程.

显然$(\frac{1}{P})=1$，$(\frac{a^2}{P})=1$，并且当$a\equiv b \pmod P$时，

$$(\frac{a}{P})=(\frac{b}{P}),$$

这是因为从$a\equiv b \pmod P$，我们有$a\equiv b \pmod{p_i}$，因而有$(\frac{a}{p_i})=(\frac{b}{p_i})$，再我们还有

定理 1 假如$(ab, P)=1$，那末

$$(\frac{ab}{P})=(\frac{a}{P})(\frac{b}{P}).$$

证明 $(\frac{ab}{P})=\prod(\frac{ab}{p_i})=\prod(\frac{a}{p_i})\cdot\prod(\frac{b}{p_i})$

$$=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$$

证毕.

与这性质对称的有：

定理 2 假设 P, Q 都是大于 1 的奇数，并且 $(a, PQ)=1$，那末

$$\left(\frac{a}{PQ}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).$$

证明 假设 $P=\prod_{i=1}^{m}p_i$, $Q=\prod_{j=1}^{n}q_j$，其中 p_i, q_j 都是质数，于是 $PQ=p_1\cdots p_m q_1\cdots q_n$，因此

$$\left(\frac{a}{PQ}\right)=\prod\left(\frac{a}{p_i}\right)\prod\left(\frac{a}{q_j}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).$$

证毕.

上面两个性质可以推广到一般几个数乘积的情况.

定理 3 $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$，$P$ 是奇数

证明 因为 $\left(\frac{-1}{P}\right)=\prod_{i=1}^{m}\left(\frac{-1}{p_i}\right)=\prod_{i=1}^{m}(-1)^{\frac{p_i-1}{2}}$

$$=(-1)^{\sum_{i=1}^{m}\frac{p_i-1}{2}}$$

下面我们用归纳法来证明下式：

$$\sum_{i=1}^{m}\frac{p_i-1}{2}\equiv\frac{P-1}{2}\pmod 2$$

即
$$\sum_{i=1}^{m}(p_i-1)\equiv P-1 \pmod 4 \qquad (1)$$

因为 p_i 都是奇数，所以 p_i-1 是偶数，于是

$$(p_1-1)(p_2-1)=p_1p_2-(p_1+p_2)+1\equiv 0 \pmod 4,$$

因此
$$(p_1-1)+(p_2-1)\equiv p_1p_2-1 \pmod 4$$

即 $m=2$ 时，（1）成立．今假定 $m-1$ 时，（1）成立，因为 p_1，…，p_{m-1} 是奇数，所以

$$\begin{aligned}\sum_{i=1}^{m}(p_i-1)&=\sum_{i=1}^{m-1}(p_i-1)+p_m-1\\&\equiv p_1\cdots p_{m-1}-1+p_m-1\\&\equiv p_1\cdots p_{m-1}p_m-1=P-1 \pmod 4\end{aligned}$$

于是（1）成立，所以定理成立．

定理 4 $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$，$P$ 是奇数．

证明 因为
$$\left(\frac{2}{P}\right)=\prod_{i=1}^{m}\left(\frac{2}{p_i}\right)=\prod_{i=1}^{m}(-1)^{\frac{p_i^2-1}{8}}$$

$$=(-1)^{\sum_{i=1}^{m}\frac{p_i^2-1}{8}},$$

与上定理 3 的证明一样，用归纳法我们容易证明

$$\sum_{i=1}^{m}(p_i^2-1)\equiv P^2-1 \pmod{16},$$

即
$$\sum_{i=1}^{m}\frac{p_i^2-1}{8}\equiv\frac{P^2-1}{8} \pmod 2,$$

于是定理成立．

定理 5 假如 P，Q 是互质的奇数，那末

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

即

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

证明 因为 $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)$

$$=\prod_i\left(\frac{Q}{p_i}\right)\prod_j\left(\frac{P}{q_j}\right)=\prod_{i,j}\left(\frac{q_j}{p_i}\right)\prod_{i,j}\left(\frac{p_i}{q_j}\right)$$

$$=\prod_{i,j}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)=\prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

$$=(-1)^{\sum\limits_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

$$=(-1)^{\left(\sum\limits_i\frac{p_i-1}{2}\right)\left(\sum\limits_j\frac{q_j-1}{2}\right)}$$

$$=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

上面这些性质除定理 2 外都是勒朗德符号具备的.

例 1 求 $\left(\frac{429}{563}\right)$，其中 563 是质数.

解 把 $\left(\frac{429}{563}\right)$ 看成亚可比符号，我们有

$$\left(\frac{429}{563}\right)=(-1)^{\frac{429-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{429}\right)=\left(\frac{563}{429}\right)=\left(\frac{134}{429}\right)$$

$$=\left(\frac{2}{429}\right)\left(\frac{67}{429}\right)=(-1)^{\frac{429^2-1}{8}}\left(\frac{67}{429}\right)$$

$$= -\left(\frac{67}{429}\right) = -(-1)^{\frac{67-1}{2}\cdot\frac{429-1}{2}}\left(\frac{429}{67}\right)$$

$$= -\left(\frac{429}{67}\right) = -\left(\frac{27}{67}\right) = -(-1)^{\frac{27-1}{2}\cdot\frac{67-1}{2}}\left(\frac{67}{27}\right)$$

$$= \left(\frac{67}{27}\right) = \left(\frac{13}{27}\right) = (-1)^{\frac{27-1}{2}\cdot\frac{13-1}{2}}\left(\frac{27}{13}\right)$$

$$= \left(\frac{1}{13}\right) = 1.$$

即 429 是 563 的平方剩余. 解毕.

这样把勒朗德符号看成亚可比符号来计算，就没有必要判别分子是否是质数，因而计算得到简化.

例 2 求所有与 30 互质的奇数 P 使

$$\left(\frac{30}{P}\right) = +1 \text{ 或 } \left(\frac{30}{P}\right) = -1.$$

解 因为

$$\left(\frac{30}{P}\right) = (-1)^{\frac{P^2-1}{8}}\left(\frac{15}{P}\right) = (-1)^{\frac{P^2-1}{8}+\frac{P-1}{2}}\left(\frac{P}{15}\right)$$

因此当

$$\left(\frac{P}{15}\right) = +1,\quad \frac{P^2-1}{8} + \frac{P-1}{2} \equiv 0 \pmod 2$$

或
$$\left(\frac{P}{15}\right) = -1,\quad \frac{P^2-1}{8} + \frac{P-1}{2} \equiv 1 \pmod 2$$

时，
$$\left(\frac{30}{P}\right) = +1.$$

根据定义我们容易得知

当 $\left(\frac{P}{15}\right) = +1$ 时， $P \equiv 1, 2, 4, 8 \pmod{15}$；

当 $\left(\frac{P}{15}\right) = -1$ 时， $P \equiv 7, 11, 13, 14 \pmod{15}$.

再同定理 7 的证明中一样，我们可以证明

当$\frac{P^2-1}{8}+\frac{P-1}{2}\equiv 0 \pmod 2$时，$P\equiv 1,3 \pmod 8$，

当$\frac{P^2-1}{8}+\frac{P-1}{2}\equiv 1 \pmod 2$时，$P\equiv 5,7 \pmod 8$.

于是解下面16个一次同余方程组：

$P\equiv 1,\ 2,\ 4,\ 8 \pmod{15}$，　　$P\equiv 1,\ 3 \pmod 8$；

$P\equiv 7,\ 11,\ 13,\ 14 \pmod{15}$，$P\equiv 5,\ 7 \pmod 8$

就得到使$\left(\frac{30}{P}\right)=+1$的16个数：

$P\equiv 1,\ 7,\ 13,\ 17,\ 19,\ 29,\ 37,\ 49,\ 71,$

$83,\ 91,\ 101,\ 103,\ 107,\ 113,\ 119 \pmod{120}$

同样使$\left(\frac{30}{P}\right)=-1$的16个数是

$P\equiv 11,\ 23,\ 31,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,$

$67,\ 73,\ 77,\ 79,\ 89,\ 97,\ 109 \pmod{120}$

习 题 5.3

把上节习题1中下列各勒朗德符号作为亚可比符号重新计算：

1. $\left(\frac{88}{109}\right)$；　　2. $\left(\frac{365}{1847}\right)$；　　3. $\left(\frac{-1457}{2389}\right)$.

4. 请把例2证明中计算详细重做一遍，校核其中数字有无错误.

§5.4　质数模的二次同余方程

现在来讨论我们的第二个问题，我们来解

$$x^2 \equiv a \pmod p, \quad p \nmid a, \quad p \text{ 是奇质数}, \tag{1}$$

上二节我们只是讨论它是否有解，在§3·3中我们也曾提到求解质数模的高次同余方程，但只是一般原则，这节我们要给出具体的求解方法.

我们知道当$\left(\frac{a}{p}\right)=1$时，由欧拉定理我们有

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p,$$

于是
$$a^{\frac{1}{2}(p-1)} \cdot a = a^{\frac{1}{2}(p+1)} \equiv a \pmod p,$$

假如$k=\frac{1}{4}(p+1)$是整数，那末$(a^k)^2 \equiv a \pmod p$，因此$x \equiv \pm a^k$就是所求解. 当k是整数时，如果它是奇数，那末$\frac{1}{4}(p+1) \equiv 1 \pmod 2$，即$p \equiv 3 \pmod 8$，如果它是偶数，那末$\frac{1}{4}(p+1) \equiv 0 \pmod 2$，即$p \equiv 7 \pmod 8$，这就是说当$p \equiv 3$或$p \equiv 7 \pmod 8$时，(1)有解. 它的解是

$$x \equiv \pm a^{\frac{1}{4}(p+1)} \pmod p.$$

例 1 解$x^2 \equiv 11 \pmod{43}$.

解 因为$\left(\frac{11}{43}\right) = -\left(\frac{43}{11}\right) = -\left(\frac{-1}{11}\right) = +1$

所以同余方程有解，这时$p=43 \equiv 3 \pmod 8$，因此所求解为

$$x \equiv \pm 11^{\frac{1}{4}(p+1)} = \pm 11^{11} \pmod{43}$$

由计算得

$11^2 = 121 \equiv -8 \pmod{43}$，$11^4 \equiv 64 \equiv 21 \pmod{43}$

$11^8 \equiv 441 \equiv 11 \pmod{43}$，$11^{10} \equiv -88 \equiv -2 \pmod{43}$，

$11^{11} \equiv -22 \equiv 21 \pmod{43}$，

所以 $$x\equiv\pm 21 \pmod{43}.$$

假如 $k=\frac{1}{4}(p+1)$ 不是整数，上法当然不能用，但我们仍然可以按它的原则来处理，因为 p 是奇质数，所以关于模8，只有下列四种情况

$$p\equiv 1,\quad p\equiv 3,\quad p\equiv 5,\quad p\equiv 7 \pmod 8.$$

上面已讨论了二种情况，下面我们来讨论其他二种，我们先讨论 $p\equiv 5 \pmod 8$ 的情况

因为 $p\equiv 5 \pmod 8$ 时，$\frac{1}{4}(p-1)$ 是整数，由

$$a^{\frac{1}{2}(p-1)}\equiv 1 \pmod p,$$

我们有 $$\left(a^{\frac{1}{4}(p-1)}-1\right)\left(a^{\frac{1}{4}(p-1)}+1\right)\equiv 0 \pmod p$$

因此

$$a^{\frac{1}{4}(p-1)}-1\equiv 0 \pmod p \text{ 或 } a^{\frac{1}{4}(p-1)}+1\equiv 0 \pmod p,$$

假如前式成立，那末

$$a^{\frac{1}{4}(p-1)}\cdot a\equiv a \pmod p,$$

即 $$a^{\frac{1}{4}(p+3)}\equiv a \pmod p,$$

显然这时 $\frac{1}{8}(p+3)$ 是整数，所以这时(1)的解是

$$x\equiv\pm a^{\frac{1}{8}(p+3)} \pmod p,$$

假如后式成立，那末

$$a^{\frac{1}{4}(p+3)}\equiv -a \pmod p,$$

由§5.2定理6，这时2是 p 的平方非剩余，即

$$2^{\frac{1}{2}(p-1)}\equiv -1 \pmod p,$$

于是

$$2^{\frac{1}{2}(p-1)}\cdot a^{\frac{1}{4}(p+3)}\equiv a \pmod p,$$

所以这时(1)的解是

$$x\equiv \pm 2^{\frac{1}{4}(p-1)}\cdot a^{\frac{1}{8}(p+3)} \pmod p.$$

这就是说当 $p\equiv 5 \pmod 8$ 时，如果 $a^{\frac{1}{4}(p-1)}\equiv 1 \pmod p$，(1)的解是

$$x\equiv \pm a^{\frac{1}{8}(p+3)} \pmod p;$$

如果 $a^{\frac{1}{4}(p-1)}\equiv -1 \pmod p$，(1)的解是

$$x\equiv \pm 2^{\frac{1}{4}(p-1)} a^{\frac{1}{8}(p+3)} \pmod p.$$

例 2　解　$x^2\equiv 23 \pmod{101}$.

解　因为 $\left(\frac{23}{101}\right)=\left(\frac{101}{23}\right)=\left(\frac{9}{23}\right)=+1$,

所以同余方程有解，这时

$$p=101\equiv 5 \pmod 8,\quad \frac{1}{4}(p-1)=25$$

我们先计算 23^{25},

$$23^2=529\equiv 24,\qquad 23^4\equiv 576\equiv -30,$$

$$23^{12}\equiv -27000\equiv -33,\quad 23^{13}\equiv -759\equiv 49$$

$$23^{25}\equiv -1617\equiv -1.$$

再计算 2^{25},

$$2^5=32,\quad 2^{10}=1024\equiv 14,$$

$$2^{20}\equiv 196\equiv -6,\qquad 2^{25}\equiv -192\equiv 10$$

因此所求解

$$x\equiv \pm 10\cdot 49=\pm 490\equiv \pm 15 \pmod{101}.$$

最后我们来讨论 $p\equiv 1 \pmod 8$ 的情况．它比前面三种

情况复杂，没有一般结论，下面介绍的，只不过是一个求解的原则而已.

我们命 $p=2^k h+1$，$k\geqq 3$，h 是奇数，由

$$a^{\frac{1}{2}(p-1)}-1=(a^{\frac{1}{4}(p-1)}-1)(a^{\frac{1}{4}(p-1)}+1)\equiv 0 \pmod p,$$

我们有

$$a^{\frac{1}{4}(p-1)}\equiv 1 \quad \text{或} \quad a^{\frac{1}{4}(p-1)}\equiv -1 \pmod p,$$

即

$$a^{2^{k-2}h}\equiv 1 \quad \text{或} \quad a^{2^{k-2}h}\equiv -1 \pmod p, \tag{2}$$

假如前式成立，我们可以再分解为

$$(a^{2^{k-3}h}-1)(a^{2^{k-3}h}+1)\equiv 0 \pmod p,$$

因此

$$a^{2^{k-3}h}\equiv 1 \quad \text{或} \quad a^{2^{k-3}h}\equiv -1 \pmod p,$$

又假如前式成立，我们又有

$$a^{2^{k-4}h}\equiv 1 \quad \text{或} \quad a^{2^{k-4}h}\equiv -1 \pmod p$$

这样如果每回都是与 1 同余的式成立，我们这样继续分解下去，经过 k 回后，a 的乘幂就降低为 h，这时 $a^h\equiv 1 \pmod p$，于是 $a^{h+1}\equiv a \pmod p$，因此这时 (1) 的解是

$$x\equiv \pm a^{\frac{1}{2}(h+1)} \pmod p.$$

假如 (2) 的后式成立，即 $a^{2^{k-2}h}\equiv -1 \pmod p$，我们在 p 的简化剩余系中，任取 p 的一个平方非剩余 b，因为

$$b^{\frac{1}{2}(p-1)}\equiv -1 \pmod p,$$

所以

$$b^{2^{k-1}h}\equiv -1 \pmod p, \tag{3}$$

于是我们有

$$b^{2^{k-1}h}\cdot a^{2^{k-2}h}\equiv 1 \pmod{p},$$

这时 b 的乘幂是 2^{k-1} 的倍数而 a 的乘幂是 2^{k-2} 的倍数，把上式再分解，我们又有

$$b^{2^{k-2}h}a^{2^{k-3}h}\equiv 1 \quad 或 \quad b^{2^{k-2}h}a^{2^{k-3}h}\equiv -1 \pmod{p},$$

假如这时又是后式成立，我们又用 (3) 式乘它就得到同余式

$$b^{2^{k-2}s}a^{2^{k-3}h}\equiv 1 \pmod{p},$$

我们再继续分解，继续把 a 的乘幂降低，因为每分解一回，a 的乘幂中及 b 的乘幂中 2 的个数都同时减少 1，因此经过若干回后，我们终可得到

$$b^{2t}a^{h}\equiv 1 \pmod{p}$$

于是 $b^{2t}a^{h+1}\equiv a \pmod{p}$，所以这时 (1) 的解是

$$x\equiv \pm b^{t}a^{\frac{1}{2}(h+1)} \pmod{p}.$$

例 3 解 $x^2\equiv 5 \pmod{41}$.

解 因为 $\left(\frac{5}{41}\right)=1$，所以同余方程有解，这时 $p=41=2^3\cdot 5+1$，$k=3$，$h=5$，由计算，我们得

$$5^{2\cdot 5}\equiv 40\equiv -1 \pmod{41}.$$

又我们容易验证 $\left(\frac{3}{41}\right)=-1$，即 3 是 41 的平方非剩余，因此

$$3^{2^2\cdot 5}\equiv -1 \pmod{41},$$

两式相乘得

$$3^{2^2\cdot 5}\cdot 5^{2\cdot 5}\equiv 1 \pmod{41},$$

再由计算

$$3^{2\cdot 5}\cdot 5^{5}\equiv 9\times 9\equiv -1 \pmod{41},$$

因此我们又得

$$3^{2^2\cdot 5}\,3^{2\cdot 5}\cdot 5^5\equiv 1\pmod{41},$$

即

$$3^{2\cdot 15}\cdot 5^5\equiv 1\pmod{41},$$

于是

$$3^{2\cdot 15}\cdot 5^6\equiv 5\pmod{41},$$

因此所求解

$$x\equiv\pm 3^{15}\cdot 5^5\equiv\pm 2\times 14=\pm 28\equiv\mp 13\pmod{41}.$$

上面的解法原则上与 $p\equiv 5\pmod 8$ 时的一样，逐步降低 k，但当 k 较大时，计算非常麻烦，下面介绍的逐步舍弃法较为简便．当然不论 p 属何形状，这法都可适用，但当 $p\not\equiv 1\pmod 8$ 时，上面已有公式，引用公式，困难一般不比这大，因此这法主要是在 $p\equiv 1\pmod 8$ 情况下采用．

我们知道(1)只有二个解，假如求得其一，他一立得．我们把 p 的简化剩余系中数代入试验当然可以求得其解，只是当 k 较大时，简化剩余系中数过多，一一代入，计算很烦，假如我们能够判别其中某些数一定不是它的解，我们就可以不经过代入验证就可把它舍弃，如果舍弃的数愈多，那末用以代入试验的数就愈少，因此不必费很大计算就可以把(1)的解求出，这就是所谓**逐步舍弃法**，具体步骤如下：

首先 p 的简化剩余系我们取绝对值最小的，即 ± 1，± 2，…，$\pm\frac{1}{2}(p-1)$，因此在 1 与 $\frac{1}{2}(p-1)$ 之间，(1)必有解，即 $0<x<\frac{1}{2}p$．再因为(1)与不定方程 $x^2=a+py$ 等价，因为 $py=x^2-a<\frac{1}{4}p^2$，所以 $y<\frac{1}{4}p$，又因为 $x^2=a+py<p(1+y)$，所以 $1+y>0$，即 $y>-1$，但 y 是整数，

所以 $y\geqq 0$，再因为 a 不是某数的平方，所以 $y>0$，于是我们有

$$0<y<\frac{1}{4}p,$$

这就是说在小于 $\frac{1}{4}p$ 的正数中，求出使 $a+py$ 成为某平方数的 y 就得到(1)的解了，因此求 x 的问题转化为求 y 的问题，y 的个数比 x 的减少了一半，这样，简化了计算.

此外我们还有下面更多的舍弃.

假如 $a+py\equiv c(\bmod q)$，而 c 是 q 的平方非剩余，那末 $a+py$ 就不是平方数，因此这样的 y 都不是我们需要的，可以舍去. 于是任取与 p 不同的奇质数 q，求出它的平方非剩余 c_1，c_2，…，c_k，$k=\frac{1}{2}(q-1)$. 再解同余方程

$$a+py\equiv c_i(\bmod q),\quad i=1,\ \cdots,\ k,$$

得 $y\equiv a_i(\bmod q)$，因此在 $<\frac{1}{4}p$ 的正数中，所有这样的

$$y=a_i+qt,\quad i=1,\ \cdots,\ k,$$

都应舍弃，毋须代入试验.

象这样取不同的 q 逐步舍弃，待所剩的个数较少，而计算不太麻烦时，即代入验证，就很容易把(1)解出.

例 4 解 $x^2\equiv 73(\bmod 127)$.

解 因为 $\left(\frac{73}{127}\right)=1$，所以同余方程有解，今用逐步舍弃法求解，这时 $a=73$，$p=127$，$\left[\frac{127}{4}\right]=31$.

首先取 $q=3$，显然 2 是 3 的平方非剩余，解同余方程

$$73+127y\equiv 2(\bmod 3),$$

得 $y\equiv 1 \pmod 3$，于是在1与31之间，删去所有形状象 $1+3t$ 的数，剩下的数是

$$2,\ 3,\ 5,\ 6,\ 8,\ 9,\ 11,\ 12,\ 14,\ 15,\ 17,$$
$$18,\ 20,\ 21,\ 23,\ 24,\ 26,\ 27,\ 29,\ 30.$$

再取 $q=5$，因为 $\left(\frac{2}{5}\right)=\left(\frac{3}{5}\right)=-1$，解同余方程

$$73+127y_1\equiv 2,\quad 73+127y_2\equiv 3 \pmod 5$$

得 $y_1\equiv 2$，$y_2\equiv 0 \pmod 5$. 于是又将所有形状象 $2+5t$，$5t$ 的数删去，剩下有

$$3,\ 6,\ 8,\ 9,\ 11,\ 14,\ 18,\ 21,\ 23,\ 24,\ 26,\ 29.$$

又取 $q=7$，因为 $\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{6}{7}\right)=-1$，并且

$73+127y_1\equiv 3$，　$73+127y_2\equiv 5$，　$73+127y_3\equiv 6 \pmod 7$ 的解分别为 $y_1\equiv 0$，$y_2\equiv 2$，$y_3\equiv 3 \pmod 7$，因此删去所有形状象 $7t, 2+7t$，$3+7t$ 的数后，就只剩下六个数

$$6,\ 8,\ 11,\ 18,\ 26,\ 29$$

代入试验，由

$$73+127\times 8=1089=33^2,$$

得知所求解是

$$x\equiv \pm 33 \pmod{127}.$$

习　题　5.4

解下列各同余方程

1. $x^2\equiv 5 \pmod{19}$；
2. $x^2\equiv 5 \pmod{29}$；
3. $x^2\equiv 2 \pmod{71}$；

4. $x^2 \equiv 3 \pmod{73}$;

5. $x^2 \equiv 11 \pmod{353}$;

6. $x^2 \equiv 13 \pmod{27}$.

§5.5 合数模的二次同余方程

这节我们讨论一般合数模的二次二项同余方程，也就是讨论它有解的条件，解的个数以及如何求解等问题.

我们先讨论模是奇质数幂的同余方程

$$x^2 \equiv a \pmod{p^k},\quad p \nmid a,\quad p\text{ 是奇质数} \tag{1}$$

假如(1)有解，那末

$$x^2 \equiv a \pmod{p} \tag{2}$$

有解，即 $\left(\frac{a}{p}\right) = +1$. 反过来假如(2)有解，即 $\left(\frac{a}{p}\right) = +1$，因为这时 $f(x) = x^2 - a$, $f'(x) = 2x$, 因此当 $p \mid f(x_1)$ 时，$p \nmid f'(x_1)$，于是我们可以根据§4.3给出的方法求出(1)的解. 再因为(2)有解时，只有二个解，所以这时(1)也只有二个解，假如 $x \equiv a \pmod{p^k}$ 是(1)的一个解，显然另一个解就是 $x \equiv -a \pmod{p^k}$，于是我们有：

定理 1 (1)有解的必要充分条件是

$$\left(\frac{a}{p}\right) = +1,$$

这时它的二个解是 $x \equiv \pm a \pmod{p^k}$，并且可以用§4.3的方法求解.

例 1 解同余方程 $x^2 \equiv 11 \pmod{125}$.

解 从同余方程 $x^2 \equiv 11 \pmod{5}$ 得 $x \equiv 1 \pmod{5}$，再从

$(1+5t_1)^2\equiv 11 \pmod{5^2}$，得 $10t_1\equiv 10 \pmod{5^2}$，因此 $t_1\equiv 1 \pmod 5$，于是 $1+5t_1\equiv 6 \pmod{5^2}$ 是 $x^2\equiv 11 \pmod{5^2}$ 的解. 又从 $(6+5^2t_2)^2\equiv 11 \pmod{5^3}$，得 $300t_2\equiv -25 \pmod{5^3}$，因此 $12t_2\equiv -1 \pmod 5$，即 $t_2\equiv 2 \pmod 5$，所以 $x=6+5^2\cdot 2=56$ 是所给方程组的一个解，于是所求解为

$$x\equiv \pm 56 \pmod{125}.$$

下面我们来讨论

$$x^2\equiv a \pmod{2^k},\quad 2\nmid a \tag{3}$$

这时不论在解的个数上或在求解的方法上都与上面模是奇质数幂的情况不完全一样.

当 $k=1$ 时，$a\equiv 1 \pmod 2$，这时(3)显然只有唯一个解 $x\equiv 1 \pmod 2$. 当 $k=2$ 时，$a\equiv 1$ 或 $a\equiv -1 \pmod 4$，因为任何奇数的平方关于模 4 必与 1 同余，因此当 $a\equiv 1 \pmod 4$ 时(3)有二个解 $x\equiv 1, 3 \pmod 4$，当 $a\equiv 3 \pmod 4$ 时，(3)无解.

当 $k=3$ 时，假如(3)有解，这解必为奇数，但任何奇数的平方关于模 8 必与 1 同余，所以 $x^2\equiv 1 \pmod 8$，因此 $a\equiv 1 \pmod 8$，这就是说 $a\equiv 1 \pmod 8$ 是(3)有解的必要条件. 反过来，假如 $a\equiv 1 \pmod 8$，因为任何奇数的平方关于模 8 都与 1 同余，所以这时，(3)有解，并且 $x\equiv 1, 3, 5, 7 \pmod{2^3}$ 是它的解.

下面我们用归纳法来证明，当 $k>3$ 时，(3)也有这样的 4 个解. 假如 $x\equiv \alpha \pmod{2^{k-1}}$ 是

$$x^2\equiv a \pmod{2^{k-1}} \tag{4}$$

的解，即 $\alpha^2-a=2^{k-1}h$，我们不妨设 $x=\alpha+2^{k-2}t$ (不能象§4.3中那样命 $x=\alpha+2^{k-1}t$)，代入(3)得

$$x^2-a=(a+2^{k-2}t)^2-a=a^2-a+2^{k-1}at+2^{2(k-2)}t^2$$
$$=2^{k-1}(h+at)+2^{2(k-2)}t^2,$$

因为$k-1\geqq 3$，所以$k-2\geqq 2$，于是

$$2(k-2)=k-2+k-2\geqq k-2+2=k$$

因此

$$x^2-a\equiv 2^{k-1}(h+at)\pmod{2^k},$$

但a是奇数，所以有适合$h+at\equiv 0\pmod 2$的唯一值t_1，于是$x\equiv a+2^{k-2}t_1\pmod{2^k}$就是(3)的解，也就是说在求得$a$后，从$a^2-a=2^{k-1}h$得到$h$，再解$h+at\equiv 0\pmod 2$得出$t_1$，于是$x\equiv\alpha+2^{k-2}t_1\pmod{2^k}$就是(3)的解了.

在求得(3)的一个解$x\equiv\alpha\pmod{2^k}$后，(3)的全部解也就求得了，这是因为假如$x\equiv\beta\pmod{2^k}$是(3)的一解，由$\beta^2\equiv\alpha^2\pmod{2^k}$，我们有$(\beta-\alpha)(\beta+\alpha)\equiv 0\pmod{2^k}$，即

$$\frac{\beta-\alpha}{2}\cdot\frac{\beta+\alpha}{2}\equiv 0\pmod{2^{k-2}},$$

但$\frac{\beta-\alpha}{2}+\frac{\beta+\alpha}{2}=\beta$，所以$\frac{\beta-\alpha}{2}$，$\frac{\beta+\alpha}{2}$中一是奇数，一是偶数，因此

$$\frac{\beta-\alpha}{2}\equiv 0\quad\text{或}\quad\frac{\beta+\alpha}{2}\equiv 0\pmod{2^{k-2}},$$

即

$$\beta\equiv\alpha\quad\text{或}\quad\beta\equiv-\alpha\pmod{2^{k-1}}$$

所以

$$\beta=\alpha+2^{k-1}t\quad\text{或}\quad\beta=-\alpha+2^{k-1}t$$

这就是说关于模2^k，β不外是下面形状的4个数

$$\alpha,\ \alpha+2^{k-1},\ -\alpha,\ -\alpha+2^{k-1},$$

显然这4个数都是(3)的解，因此它就是(3)的全部解.

综合上述得：

定理 2 同余方程

$$x^2 \equiv a \pmod{2^k},\ 2\nmid a. \tag{3}$$

当 $k=1$ 时有唯一个解 $x\equiv 1 \pmod 2$；当 $k=2$ 时，有解的必要充分条件是 $a\equiv 1 \pmod 4$，这时它有 2 个解

$$x\equiv 1,\ 3 \pmod 4;$$

当 $k\geq 3$ 时，有解的必要充分条件是 $a\equiv 1 \pmod 8$，这时它有 4 个解，假如 $x\equiv \alpha \pmod{2^k}$ 是它的一个解，那末它的全部解是

$$x\equiv \pm\alpha,\ \pm\alpha+2^{k-1} \pmod{2^k}.$$

要注意的是在用 § 4.3 中方法求解 (1) 或 (3) 时，假如能用视察法或根据已知结果求得 $x^2\equiv a \pmod{p^{k_1}}$ 或 $x^2\equiv a \pmod{2^{k_1}}$ 的一个解，我们就可从这同余方程开始，这样在计算上就简化多了．因为我们只要求得 (1) 或 (3) 一个解，那末 (1) 或 (3) 的全部解也就求得．

例 2 解 $x^2\equiv 57 \pmod{64}$.

解 这里 $64=2^6, k=6$，$57\equiv 1 \pmod 8$，所以同余方程有解，我们不难知道 $x\equiv 5 \pmod{2^5}$ 是

$$x^2\equiv 57 \pmod{2^5},$$

的解，因此这时 $\alpha=5$，$25-57=2^5(-1), h=-1$，解 $5t_3-1\equiv 0 \pmod 2$ 得 $t_3\equiv 1 \pmod 2$，所以 $x_3=5+2^4\cdot 1=21$ 是所给同余方程的解，于是所求的 4 个解是

$$x\equiv \pm 21,\ \pm 21+32\equiv \pm 53 \pmod{64}.$$

运算熟练的读者不难会想到 $57+64=121=11^2$，于是原同余方程可以写成 $x^2\equiv 11^2 \pmod{64}$，因此 $x\equiv \pm 11\equiv \mp 53 \pmod{64}$ 就是它的解．

例 3 假定 α 是 $x^2\equiv a(\mathrm{mod}\ 2^k)$ 的解，这里 $k\geqslant 3$，$2\nmid a$，那末 α 与 $\alpha+2^{k-1}$ 两数中有一且仅有一是 $x^2\equiv a\ (\mathrm{mod}\ 2^{k+1})$ 的解。

证 设 $\alpha^2-a=2^k t$，那末

$(\alpha+2^{k-1})^2-a=(\alpha^2-a)+2^k\alpha+2^{2k-2}=2^k(t+\alpha+2^{k-2})$，

但 t 与 $t+\alpha+2^{k-2}$ 的和是奇数，因此这两数一为奇一为偶，即 α 与 $\alpha+2^{k-1}$ 中有一且仅有一是 $x^2\equiv a\ (\mathrm{mod}\ 2^{k+1})$ 的解，证毕。

引用这结果逐步求 $x^2\equiv a(\mathrm{mod}\ 2^k)$ 的解时较方便。

对于一般合数模的二次二项同余方程，由上面的定理及§4.3我们有

定理 3 假定 $m=2^{m_0}p_1^{m_1}\cdots p_k^{m_k}$，$p_i$ 是奇质数，那末同余方程

$$x^2\equiv a(\mathrm{mod}\ m),\quad (a,\ m)=1$$

有解的必要充分条件是

$$\left(\frac{a}{p_i}\right)=1,\qquad i=1,\ 2,\ \cdots,\ k,$$

并且当 $m_0=2$ 时，$a\equiv 1\ (\mathrm{mod}\ 4)$，当 $m_0\geqq 3$ 时 $a\equiv 1\ (\mathrm{mod}\ 8)$。假如上面的条件成立，那末解的个数当 $m_0=0$，1 时是 2^k，当 $m_0=2$ 时是 2^{k+1}，当 $m_0\geqq 3$ 时是 2^{k+2}。

我们的第二个问题到此已完全解答了。

习 题 5.5

解下列各同余方程：

1. $x^2\equiv 41\ (\mathrm{mod}\ 64)$；
2. $x^2\equiv 2\ (\mathrm{mod}\ 7^3)$；

3. $x^2 \equiv 145 \pmod{256}$;

4. $x^2 \equiv 69 \pmod{508}$.

5. 凡是(3)的解都是(4)的解，但是(3)的全部解是否就是(4)的全部解？试举例说明.

第六章　原根与指标

以前的讨论直接间接都与简化剩余系有关，因此假如简化剩余系能够很简单的表出，那末很多问题就容易得到简化，这样就需要我们引进原根．这章我们讨论原根的存在，求法，简化剩余系的构造以及与它有关的指标等问题．

§6.1　阶　　数

我们知道当 $(a, m)=1$ 时，由欧拉定理有 $a^{\varphi(m)}\equiv 1 \pmod m$，这就是说任意与 m 互质的整数 a 自乘到某次幂就要关于模 m 与 1 同余，因此有正整数 λ 存在，使

$$a^{\lambda}\equiv 1 \pmod m,$$

并且

$$a^{k}\not\equiv 1 \pmod m,\quad 0<k<\lambda,$$

这最小正整数 λ，叫做 a 关于模 m 的阶数，显然 $\lambda\leq\varphi(m)$，由 §2.2 例 1，我们又得知 $\lambda\mid\varphi(m)$．

假如 $\lambda=\varphi(m)$，也就是说 a 关于模 m 的阶数是 $\varphi(m)$，那末 a 叫做 m 的原根．

譬如 $a=3$，$m=10$，这时 $\varphi(m)=4$，

$$3^1=3,\ 3^2=9,\ 3^3\equiv 7,\ 3^4\equiv 1 \pmod{10},$$

所以 3 关于 10 的阶数是 4，因此 3 是 10 的原根．又如 $a=3$，$m=8$，这时 $\varphi(m)=4$，因为 $3^2\equiv 1 \pmod 8$，所以 3 关

于 8 的阶数是 2，因此它不是 8 的原根．再因为任意奇数的平方关于模 8 都与 1 同余，所以 8 的原根不存在．

假如 a 关于 m 的阶数是 λ，那末

$$a^0,\ a^1,\ \cdots,\ a^{\lambda-1}$$

中任意二数关于 m 互不同余，这是因为如果 $a^r\equiv a^s \pmod m$，$1\leqq r<s\leqq\lambda$，那末 $a^{s-r}\equiv 1 \pmod m$，但 $s-r<\lambda$，这与 a 的阶数是 λ 的假设不合．又显然它们都与 m 互质，所以它们是 m 的简化剩余系的一部分，假如 $\lambda=\varphi(m)$ 也就是说 a 是 m 的原根，那末它们就是 m 的简化剩余系了．

下面是关于阶数的基本定理：

定理 1 假定 a 关于模 m 的阶数是 λ，那末

$$a^r\equiv a^s \pmod m$$

的必要充分条件是

$$r\equiv s \pmod \lambda.$$

证明 充分条件显然成立，下面我们只证明它是必要条件．

命 $r=q_1\lambda+r'$，$s=q_2\lambda+s'$，$0\leqq r'$，$s'<\lambda$，

因为 $\quad a^r=(a^\lambda)^{q_1}\cdot a^{r'}\equiv a^{r'}$，$a^s\equiv a^{s'} \pmod m$，

所以 $$a^{r'}\equiv a^{s'} \pmod m,$$

即 $$a^{r'-s'}\equiv 1 \pmod m.$$

因此 $r'=s'$，于是 $r\equiv s \pmod \lambda$，这就是说必要条件成立，所以定理得证．

特别，当 a 是 m 的原根时，$a^r\equiv a^s \pmod m$ 的必要充分条件是 $r\equiv s(\bmod\ \varphi(m))$．

定理 2 假定关于模 m，a 的阶是 λ，那末 a^k 的阶也是 λ 的必要充分条件是 $(k,\ \lambda)=1$．

证明 假定$(k, \lambda)=1$，a^k的阶数是t，因为

$$(a^k)^\lambda=(a^\lambda)^k\equiv 1 \pmod m,$$

所以$t\mid\lambda$，又因为

$$(a^k)^t=a^{kt}\equiv 1 \pmod m,$$

所以$\lambda\mid kt$，因为$(k, \lambda)=1$，所以$\lambda\mid t$，于是$t=\lambda$.

再假如a及a^k的阶数都是λ，$(k, \lambda)=d$，因为

$$(a^k)^{\frac{\lambda}{d}}=(a^\lambda)^{\frac{k}{d}}\equiv 1 \pmod m,$$

所以 $\lambda\mid\dfrac{\lambda}{d}$，因此$d=1$，即$(k, \lambda)=1$.

证毕.

定理 3 假定a，b关于模m的阶数分别是λ，μ，如果$(\lambda, \mu)=1$，那末ab关于模m的阶数是$\lambda\mu$.

证明 假定ab关于m的阶数是k，因为$a^\lambda\equiv 1$，$b^\mu\equiv 1 \pmod m$，于是

$$(ab)^{\lambda\mu}=(a^\lambda)^\mu(b^\mu)^\lambda\equiv 1 \pmod m.$$

所以$k\mid\lambda\mu$，又因为

$$(ab)^{k\lambda}=(a^\lambda)^k b^{k\lambda}\equiv b^{k\lambda}\equiv 1 \pmod m.$$

所以$\mu\mid k\lambda$，但$(\lambda, \mu)=1$， 因此$\mu\mid k$. 同样$\lambda\mid k$， 于是$\lambda\mu\mid k$，所以$k=\lambda\mu$，因此定理得证.

奇质数p的原根的偶数幂当然是p的平方剩余，但是p的平方剩余也只有这些.

例 1 假定a是奇质数p的原根，那末a的奇数幂是p的平方非剩余.

证 用反证法，如果a^{2k+1}是p的平方剩余，那末

$$(a^{2k+1})^{\frac{p-1}{2}}=a^{\frac{2k+1}{2}(p-1)}\equiv 1 \pmod p$$

因为 a 是 p 的原根，所以 $\frac{2k+1}{2}$ 应该是整数，这显然是矛盾．因此根据欧拉判别法，a 是 p 的平方非剩余．证毕．

例 2　假定 p 及 $4p+1$ 都是奇质数，试证 2 是 $4p+1$ 的原根．

证　设 $q=4p+1$，所以 $\varphi(q)=4p$，因此 2 关于模 q 的阶数只能是 1，2，4，p，$2p$ 及 $4p$．因为 p 是奇数，所以 $p\equiv1(\mathrm{mod}\ 2)$，于是 $q\equiv5(\mathrm{mod}\ 8)$，由 §5.2 定理 6 得知，2 是 q 的平方非剩余，因此

$$2^{2p}\equiv-1(\mathrm{mod}\ q),$$

所以 2 关于模 q 的阶数不是 $2p$，当然也不是 $2p$ 的因子 2 及 p．显然 2 关于 q 的阶数不是 1 也不是 4，于是 2 关于 q 的阶数是 $4p$．所以 2 是 q 的原根．证毕．

习　题　6.1

1．假设 p 是奇质数，a 是大于 1 的整数，试证

1）a^p-1 的奇质因数或是 $a-1$ 的因数或是形状象 $2pm+1$ 的数；

2）a^p+1 的奇质因数或是 $a+1$ 的因数或是形状象 $2pm+1$ 的数．

2．假定 p 是奇质数，n 不是 $p-1$ 的因数，试证

$$1^n+2^n+\cdots+(p-1)^n\equiv0(\mathrm{mod}\ p).$$

3．假如 a 关于模 m 的阶数是 λ，试证 a^k 关于模 m 的阶数是 $\frac{\lambda}{(\lambda,k)}$．

4．设 p_1，p_2 是奇质数；$a\equiv a_1(\mathrm{mod}\ p_1)$，$a\equiv a_2(\mathrm{mod}\ p_2)$，

并且 a_1 关于 p_1 的阶数是 λ_1，a_2 关于 p_2 的阶数是 λ_2，试证 a 关于模 p_1p_2 的阶数是 λ_1，λ_2 的最小公倍数 $[\lambda_1, \lambda_2]$.

5. 假设质数 $p=2^m+1$，试证 p 的平方非剩余是 p 的原根.

6. 假定 p，$6p+1$ 都是奇质数，试证 3 是 p 的原根.

§ 6.2 原根存在的必要充分条件

我们知道任意数不一定都有原根，哪些数有原根其必要充分条件如何，又假如有原根它究竟有多少个原根？这是本节我们要讨论的两个问题.

我们先讨论原根存在的必要充分条件.

假定 a 是 $m=p_1^{m_1}\cdots p_k^{m_k}$ 的原根，因为 $(a, m)=1$，所以 $(a, p_i^{m_i})=1$，于是由欧拉定理，得

$$a^{\varphi(p_i^{m_i})}\equiv 1 \pmod{p_i^{m_i}},$$

假如 $l=[\varphi(p_1^{m_1}), \cdots, \varphi(p_k^{m_k})]$，那末

$$a^l\equiv 1 \pmod{p_i^{m_i}},$$

因此

$$a^l\equiv 1 \pmod{m}.$$

但 a 是 m 的原根，所以 $\varphi(m)|l$，又因为 $\varphi(m)=\varphi(p_1^{m_1})\cdots\varphi(p_k^{m_k})$ 是 l 的倍数，即 $l|\varphi(m)$，所以 $l=\varphi(m)$，即

$$[\varphi(p_1^{m_1}), \cdots, \varphi(p_k^{m_k})]=\varphi(p_1^{m_1})\cdots\varphi(p_k^{m_k}),$$

因此 $\varphi(p_1^{m_1})$，$\cdots$，$\varphi(p_k^{m_k})$ 两两互质，但

$$\varphi(2^r)=2^{r-1}, \quad \varphi(p^r)=p^{r-1}(p-1), \qquad p \text{ 是奇质数},$$

于是 m 中奇质因数不能多于 1 个，假如偶质因数，奇质因数同时存在，那末偶质因数的乘幂又不能大于 1，这就是说假

如 m 有原根，那末 m 是下面形状的数.

$$2^k,\quad p^k,\quad 2p^k.$$

但是象上面三种形状的数是否都有原根呢？下面我们来分别讨论.

1. $m=2^k$

当 $k=1$ 时 $m=2$，这时 $\varphi(m)=1$，显然 1 是它的原根，当 $k=2$ 时 $m=4$，这时 $\varphi(m)=2$，而 1，3 是 4 的简化剩余系，显然 3 是它的原根.

当 $k\geqq 3$ 时，$\varphi(m)=2^{k-1}$，而 m 的简化剩余系是由奇数组成的. 假如我们能够证明对于任意奇数 a，

$$a^{2^{k-2}}\equiv 1 \pmod{2^k} \tag{1}$$

成立，那末 $m=2^k$ 就没有原根.

下面我们用归纳法来证明(1)，因为任何奇数的平方关于模 8 与 1 同余，即 $a^2\equiv 1 \pmod{2^3}$，所以 $k=3$ 时(1)成立，今假定 $k\geqslant 3$ 时(1)成立，因为

$$a^{2^{k-1}}=(a^{2^{k-2}})^2\equiv(1+2^kt)^2\equiv 1 \pmod{2^{k+1}},$$

即对于 $k+1$，(1)也成立，所以当 $k\geqq 3$ 时(1)成立.

2. $m=p^k$

当 $k=1$ 即 $m=p$ 时，$\varphi(m)=p-1$，命

$$p-1=q_1^{k_1}\cdots q_r^{k_r},$$

假如我们能够找出关于模 p 阶数是 $q_i^{k_i}$ 的数 b_i，$i=1,\cdots,r$，那末由 §6.1 定理 3

$$q=b_1b_2\cdots b_r$$

的阶数就是 $p-1$，因此 q 就是 p 的原根了.

我们来考虑同余方程

$$x^{\frac{p-1}{q_i}}\equiv 1 \pmod p, \tag{2}$$

因为 p 是质数，所以它的不相同解的个数不大于

$$\frac{p-1}{q_i}<p-1,$$

因此在 p 的简化剩余系中必有不满足(2)的 a_i 存在，即

$$a_i^{\frac{p-1}{q_i}}\not\equiv 1 \pmod p.$$

命 $b_i=a_i^{\frac{p-1}{q_i^{k_i}}}$，下面我们来证明 b_i 关于模 p 的阶数 $\lambda_i=q_i^{k_i}$. 因为

$$b_i^{q_i^{k_i}}=\left(a_i^{\frac{p-1}{q_i^{k_i}}}\right)^{q_i^{k_i}}=a_i^{p-1}\equiv 1 \pmod p,$$

所以 $\lambda_i\mid q_i^{k_i}$，即 $\lambda_i=q_i^{l_i}$，$l_i\leqq k_i$，假如 $l_i<k_i$，因为 $b_i^{\lambda_i}\equiv 1 \pmod p$，所以

$$\left(a_i^{\frac{p-1}{q_i^{k_i}}}\right)^{\lambda_i}=\left(a_i^{\frac{p-1}{q_i^{k_i}}}\right)^{q_i^{l_i}}=a_i^{\frac{p-1}{q_i^{k_i-l_i}}}\equiv 1 \pmod p,$$

于是 $$a_i^{\frac{p-1}{q_i}}\equiv 1 \pmod p,$$

这与假设不合，因此 b_i 的阶数 $\lambda_i=q_i^{k_i}$. 即 g 是 p 的原根.

当 $k\geqq 2$ 时，假定 g 是 p 的原根，即 $g^{p-1}\equiv 1 \pmod p$，于是 $$g^{p-1}\not\equiv 1 \quad 或 \quad g^{p-1}\equiv 1 \pmod{p^2}.$$

下面我们来证明当 $g^{p-1}\not\equiv 1 \pmod{p^2}$，即 $g^{p-1}=1+ph$，$p\nmid h$ 时，g 就是 p^k 的原根. 当 $g^{p-1}\equiv 1 \pmod{p^2}$ 时，$g+p$ 是 p^k 的原根.

当 $g^{p-1}\not\equiv 1 \pmod{p^2}$ 时，假定关于模 p^k，g 的阶数是 λ，那末 $\lambda\mid\varphi(p^k)$，即 $\lambda\mid p^{k-1}(p-1)$，我们命

$$p^{k-1}(p-1)=\lambda s,$$

因为 $g^{\lambda}\equiv1(\bmod p^{k})$，所以 $g^{\lambda}\equiv1(\bmod p)$，于是 $(p-1)|\lambda$，即 $\lambda=(p-1)t$，因此

$$p^{k-1}=ts,$$

这就是说 $t=p^{e}$，$e\leq k-1$. 所以

$$\lambda=p^{e}(p-1),$$

假如 $e<k-1$，那末 $e+2\leq k$，于是 $g^{\lambda}\equiv1(\bmod p^{e+2})$，但

$$g^{\lambda}=g^{p^{e}(p-1)}=(g^{p-1})^{p^{e}}=(1+hp)^{p^{e}}$$

$$\equiv1+hp^{e+1}(\bmod p^{e+2}),$$

所以 $hp^{e+1}\equiv0(\bmod p^{e+2})$，因此 $h\equiv0(\bmod p)$，这与 $ph\not\equiv0(\bmod p^{2})$ 的假设不合，于是 $e=k-1$，所以 $\lambda=p^{k-1}(p-1)$，这就是说当 $g^{p-1}\not\equiv1(\bmod p^{2})$ 时，g 是 p 的原根.

当 $g^{p-1}\equiv1(\bmod p^{2})$ 时，因为 $g+p$ 显然也是 p 的原根，这时

$$(g+p)^{p-1}-1\equiv g^{p-1}-1+p(p-1)g^{p-2}$$

$$\equiv p(p-1)g^{p-2}(\bmod p^{2}),$$

因为 $(g,\ p)=1$，所以 $p\nmid g^{p-2}$，因此 $(q+p)^{p-1}\not\equiv1(\bmod p^{2})$，根据上面证得的结果，得知 $g+p$ 是 p^{k} 的原根，这就是说当 $g^{p-1}\equiv1(\bmod p^{2})$ 时，$g+p$ 是 p 的原根.

3. $m=2p^{k}$

这时 $\varphi(m)=\varphi(2)\varphi(p^{k})=\varphi(p^{k})$. 假定 g 是 p^{k} 的原根，那末当 g 是奇数时，g 是 m 的原根，这是因为 $(g,\ m)=1$，

$$g^{\varphi(m)}\equiv1(\bmod m).$$

假如 g 关于 m 的阶数 $\lambda<\varphi(m)$，从 $g^{\lambda}\equiv1(\bmod m)$，即得 $g^{\lambda}\equiv1(\bmod p^{k})$，这与 g 是 p^{k} 的原根的假设不合，因此 $\lambda=\varphi(m)$，于是 g 是 m 的原根.

当 g 是偶数时，因为 $g+p^k$ 也是 p^k 的原根，这时 $g+p^k$ 是奇数，所以 $g+p^k$ 是 m 的原根.

综合上面的讨论，我们有：

定理 1 $m(>1)$ 有原根的必要充分条件是它是下面形状的数

$$2,\ 2^2,\ p^k,\ 2p^k.$$

这里 p 是奇质数，k 是任意正整数.

上面虽是讨论原根的存在，但同时也是求原根的方法. 求 m 的原根的问题基本上就是求质数 p 的原根的问题. 当 p 较大时，上面求 p 的原根方法非常麻烦，首先 $\varphi(p)$ 分解为质因数的乘积不很容易，其次在 p 的简化剩余系中，求不适合(2)的数 a_i 更有困难，但是舍此，并无一般简便方法.

例 1 求 $p=41$ 的原根.

解 这时 $p-1=40=2^3\cdot5$，$\dfrac{p-1}{2}=20$，

由计算

$$3^2=9,\ 3^4=81\equiv-1,\ 3^8\equiv1,$$
$$3^{16}\equiv1,\ 3^{20}\equiv-1 \pmod{41}$$

得知 3 不是同余方程 $x^{\frac{40}{2}}=x^{20}\equiv1 \pmod{41}$ 的解，又 $\dfrac{p-1}{5}=8$，由计算

$$2^2=4,\ 2^4=16,\ 2^8=256\equiv10 \pmod{41}$$

得知 2 不是同余方程 $x^{\frac{40}{5}}=x^8\equiv1 \pmod{41}$ 的解，于是

$$3^5\cdot2^8\equiv-3\cdot10\equiv11 \pmod{41}$$

是 41 的一个原根.

例 2 求 $m=2\cdot 41^2=3362$ 的原根.

解 关于模 $41^2=1681$，由计算我们得知

$$11^2=121,\qquad 11^4=14641\equiv -488,$$
$$11^5\equiv -325,\qquad 11^{10}\equiv 105625\equiv -278,$$
$$11^{20}\equiv 77284\equiv -42,\quad 11^{40}\equiv 1764\equiv 83,$$

即 $11^{40}\not\equiv 1\ (\bmod 41^2)$，所以 11 是 41^2 的原根，又因为 11 是奇数，所以 11 也是 $m=2\cdot 41^2$ 的原根. 解毕.

最后我们来讨论原根的个数.

假定 g 是 m 的原根，那末

$$g^0,\ g^1,\ \cdots,\ g^{\varphi(m)-1} \tag{3}$$

是 m 的简化剩余系，因为 m 的原根都与 m 互质，所以 m 的原根都在(3)中. 今假定 g^i 关于 m 的阶数是 λ，即

$$(g^i)^\lambda=g^{i\lambda}\equiv 1\ (\bmod m),$$

所以 $\varphi(m)\mid i\lambda$，命 $(i,\ \varphi(m))=d$，于是 $\left.\dfrac{\varphi(m)}{d}\right|\lambda$，但

$$(g^i)^{\frac{\varphi(m)}{d}}=(g^{\varphi(m)})^{\frac{i}{d}}\equiv 1\ (\bmod m),$$

所以 $\left.\lambda\right|\dfrac{\varphi(m)}{d}$. 于是 $\lambda=\dfrac{\varphi(m)}{d}$. 因此当 $d=(i,\ \varphi(m))=1$ 时，g^i 的阶数就是 $\varphi(m)$，这就是说对于 $\varphi(m)$ 的简化剩余系中任一与 $\varphi(m)$ 互质的数 i，g^i 都是 m 的原根，于是我们有：

定理 2 假如 m 有原根，那末它有 $\varphi(\varphi(m))$ 个关于模 m 不相同的原根.

例 3 求 $p=17$ 的所有原根.

解 这时 $p-1=16=2^4$，因为

$$3^2=9,\ 3^4=81\equiv 13,\ 3^8\equiv 169\equiv 16,\ (\bmod 17)$$

所以 $3^8 \not\equiv 1 \pmod{17}$，于是 3 是 17 的原根.

再因为 $\varphi(p-1)=2^3=8$，而

$$1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15$$

是 $p-1=16$ 的简化剩余系，因此 17 的所有原根是

$$3^1=3,\quad 3^3=27\equiv 10,\quad 3^5\equiv 90\equiv 5,$$
$$3^7\equiv 45\equiv 11,\quad 3^9\equiv 99\equiv 14,\quad 3^{11}\equiv 126\equiv 7,$$
$$3^{13}\equiv 63\equiv 12,\quad 3^{15}\equiv 108\equiv 6,$$

即 3，5，6，7，10，11，12，14 等 8 个数.

习 题 6.2

1. 求下列各数的原根

$$23,\ 54,\ 529,\ 1058,$$

2. 假如 g 是 p 的平方非剩余，$p-1=2^{\alpha_0}q_1^{\alpha_1}\cdots q_k^{\alpha_k}$，如果 $g^{\frac{p-1}{q_i}}\not\equiv 1 \pmod p$，试证 g 是 p 的原根.

3. 假如质数 $p=2^k+1$，试证 p 的平方非剩余都是 p 的原根.

§6.3 简化剩余系的构造

假如数已给出，它的简化剩余系我们不难写出，但是对一般数 m 的简化剩余系的构造如何，怎样能够简单地有规则地写出？这节我们就是讨论这问题.

我们知道当 m 的原根存在时，m 的简化剩余系可以用它的原根 g 的乘幂 g^0，g^1，$\cdots$，$g^{\varphi(m)-1}$ 来表示，这是最简单的形状了. 假如 m 的原根不存在，譬如 $m=2^k(k\geqq 3)$，它们的

简化剩余系的构造应该是怎样的呢？

首先我们来讨论 $2^k(k\geqq 3)$ 的简化剩余系，在 §6.2 中，我们曾经证明当 $k\geqq 3$ 时，对于任意奇数 a，我们有

$$a^{2^{k-2}}\equiv 1\ (\mathrm{mod}\ 2^k),$$

这就是说关于模 2^k，任意奇数的阶不超过 2^{k-2}，有没有阶数恰为 2^{k-2} 的数呢？假如有，我们就可以用它的各乘幂表示 2^k 的简化剩余系的一半，至于另一半，如果能够用它们的负数来补充，那末 2^k 的简化剩余系与由原根各乘幂形成的简化剩余系基本上没有大的区别，可以说形状也是最简单的了．

定理 1 关于模 $2^k(k\geqq 3)$，5 的阶数是 2^{k-2}．

证明 假如我们能够证明当 $k\geqq 3$ 时，

$$5^{2^{k-3}}\equiv 1+2^{k-1}\ (\mathrm{mod}\ 2^k), \tag{1}$$

那末 $5^{2^{k-3}}\not\equiv 1\ (\mathrm{mod}\ 2^k)$，因此 5 关于模 2^k 的阶数是 2^{k-2}，于是定理就告成立．

我们用归纳法来证明(1)．当 $k=3$ 时(1)显然成立，用归纳法，假定 $k-1$ 时(1)成立，即

$$5^{2^{k-4}}=1+2^{k-2}+2^{k-1}t,$$

于是

$$5^{2^{k-3}}=(5^{2^{k-4}})^2\equiv(1+2^{k-2}+2^{k-1}t)^2$$

$$\equiv 1+2^{k-1}\ (\mathrm{mod}\ 2^k),$$

所以(1)成立，因此定理得证．

因为 $5\equiv 1\ (\mathrm{mod}\ 4)$，显然对于任意 i，我们有 $5^i\equiv 1\ (\mathrm{mod}\ 4)$，因此 $-5^i\equiv -1\ (\mathrm{mod}\ 4)$．于是对于任意二个不同的数 i，j，我们有 $5^i\not\equiv -5^j\ (\mathrm{mod}\ 2^k)$，这就是说在 2^{k-1} 个数

$$\pm 5^0,\ \pm 5^1,\ \cdots,\ \pm 5^{2^{h-2}-1} \tag{2}$$

中，任意二数关于模 2^h 不同余，并且其中各数又都与 2^h 互质；这样我们就有：

定理 2 (2)是 2^h 的简化剩余系.

再我们来讨论任意数 m 的简化剩余系的构造.

假定 $m = m_1 m_2$，$(m_1, m_2) = 1$，m_1，m_2 的简化剩余系分别是

$$a_1,\ \cdots,\ a_{\varphi(m_1)};\ b_1,\ \cdots,\ b_{\varphi(m_2)},$$

如果 $a_i \equiv 1 \pmod{m_2}$，$b_j \equiv 1 \pmod{m_1}$，

那末 $\varphi(m_1)\varphi(m_2) = \varphi(m)$ 个数

$$a_i b_j,\ i = 1,\ \cdots, \varphi(m_1);\ j = 1,\ \cdots, \varphi(m_2)$$

就是 $m = m_1 m_2$ 的简化剩余系，这是因为 $(a_i, m_1) = 1$，$(a_i, m_2) = 1$，所以 $(a_i, m) = 1$，同样 $(b_j, m) = 1$，于是 $(a_i b_j, m) = 1$，这就是说 $a_i b_j$ 与 m 互质，再假如

$$a_i b_j \equiv a_k b_l \pmod{m},$$

那末 $a_i b_j \equiv a_k b_l \pmod{m_1}$，因此 $a_i \equiv a_k \pmod{m_1}$，所以 $a_i = a_k$. 同样 $b_j = b_l$，这就是说 $a_i b_j$ 中任意二数关于模 m 不同余，于是 $\varphi(m)$ 个数 $a_i b_j$ 构成 m 的简化剩余系.

要注意的是上面 $a_i \equiv 1 \pmod{m_2}$ 的条件，只要适当挑选 m_1 的简化剩余系都是可以得到的，这是因为假如 x_1，x_2，$\cdots$，$x_{\varphi(m_1)}$ 是 m_1 的简化剩余系，因为同余方程

$$m_1 t \equiv 1 - x_i \pmod{m_2},$$

即 $$m_1 t + x_i \equiv 1 \pmod{m_2}$$

有唯一解 $t \equiv t_i \pmod{m_2}$，命

$$a_i = m_1 t_i + x_i,$$

显然 $a_i \equiv 1 \pmod{m_2}$ 并且 $a_i \equiv x_i \pmod{m_1}$，所以 a_1，$\cdots$，

$a_{\varphi(m_1)}$ 是 m_1 的简化剩余系.

例 引用上述方法求 $m=40$ 的简化剩余系.

解 因为 $m=40=5\times 2^3$. 我们适当取 5 及 2^3 的简化剩余系

$$1,\ 9,\ 17,\ 33;\qquad 1,\ 11,\ 21,\ 31$$

于是 40 的简化剩余系是

$1,\ 9,\ 17,\ 33,$

$11,\ 11\times 9\equiv 19,\ 11\times 17\equiv 27,\ 11\times 33\equiv 3,$

$21,\ 21\times 9\equiv 29,\ 21\times 17\equiv 37,\ 21\times 33\equiv 13,\ 31,$

$31\times 9\equiv 39,\ 31\times 17\equiv 7,\ 31\times 33\equiv 23,$

即

$$1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19,\ 21$$
$$23,\ 27,\ 29,\ 31,\ 33,\ 37,\ 39.$$

解毕.

上面 $m=m_1m_2$ 的简化剩余系的构造，在讨论某些一般问题时可能把问题简化. 假如只是求某个已知数的简化剩余系，我们可以直接根据 §2.2 中定义来求，用这方法反而麻烦. 上列正好说明这问题.

习 题 6.3

假定 $k=0$ 或 $k=1$ 时，$c=1$，$c_0=1$，$k\geqq 2$ 时，$c=2$，$c_0=2^{k-2}$. 试证

1. $(-1)^i 5^j$，$i=0,\ 1,\ \cdots,\ c-1$；$j=0,\ 1,\cdots,\ c_0-1$ 是 2^k 的简化剩余系；

2. $(-1)^i 5^j\equiv(-1)^{i'}5^{j'}\pmod{2^k}$ 的必要充分条件是

$$i\equiv i'\pmod{c},\quad j\equiv j'\pmod{c_0}.$$

§6.4 指　　标

引用原根，我们可以引进一个新概念，它与中学代数中对数类似.

假定 g 是 m 的原根，那末 1，g，g^2，…，$g^{\varphi(m)-1}$ 是 m 的简化剩余系，于是任一与 m 互质的数 a 必与 g 的某乘幂 g^e 同余，即

$$g^e \equiv a(\bmod m),\quad 0 \leqq e \leqq \varphi(m)-1,$$

这对已知 m，g，由 a 唯一决定的 e，叫做关于模 m 以 g 为底 a 的指标，用

$$e = \operatorname{ind}_g a$$

表示，假如省去底 g 不致有误会，我们又常常简写成

$$e = \operatorname{ind} a.$$

譬如 $g=2$ 是 $p=13$ 的原根，由计算我们有

$g^0=1$，$g^1=2$，$g^2=4$，$g^3=8$，$g^4\equiv 3$，$g^5\equiv 6$，

$g^6\equiv 12$，$g^7\equiv 11$，$g^8\equiv 9$，$g^9\equiv 5$，$g^{10}\equiv 10$，$g^{11}\equiv 7$.

因此得对于模 13，底是 2 的指标表如下：

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} a$	0	1	4	2	9	5	11	3	8	10	7	6

要注意的是 a 的指标与模 m 有关也与底 g 有关，譬如 2，3 都是 5 的原根，$\operatorname{ind}_3 3=1$，而 $\operatorname{ind}_2 3=3$.

显然，$\operatorname{ind} 1=0$，$\operatorname{ind} g=1$，并且由 §6.1 定理 1，我们得 $a\equiv b(\bmod m)$ 成立的必要充分条件是

$$\text{ind}\, a \equiv \text{ind}\, b \pmod{\varphi(m)}.$$

下面是指标的基本性质，它与对数的性质类似，根据定义容易验证，读者试作为习题加以补充.

$$\text{ind}\, ab \equiv \text{ind}\, a + \text{ind}\, b \pmod{\varphi(m)},$$

$$\text{ind}\, a^n \equiv n\, \text{ind}\, a \pmod{\varphi(m)},$$

$$\text{ind}_g\, a \equiv \text{ind}_g\, k\, \text{ind}_k\, a \pmod{\varphi(m)}.$$

利用指标表解同余方程非常简便，兹用例说明如下：

例 1 解 $11x \equiv 5 \pmod{13}$.

解 取指标得

$$\text{ind}\, 11 + \text{ind}\, x \equiv \text{ind}\, 5 \pmod{12},$$

由上面的表查得 $\text{ind}\, 11 = 7$，$\text{ind}\, 5 = 9$，于是

$$7 + \text{ind}\, x \equiv 9 \pmod{12},$$

即

$$\text{ind}\, x \equiv 2 \pmod{12},$$

又由表得

$$x \equiv 4 \pmod{13}.$$

例 2 解 $5x^2 + 3x - 10 \equiv 0 \pmod{13}$.

解 因为 $8 \cdot 5 \equiv 1 \pmod{13}$，所以

$$x^2 + 24x - 80 \equiv 0 \pmod{13},$$

即

$$x^2 - 2x - 2 \equiv 0 \pmod{13},$$

也就是

$$(x-1)^2 \equiv 3 \pmod{13},$$

取指标得

$$2\, \text{ind}\, (x-1) \equiv \text{ind}\, 3 \pmod{12},$$

即

$$2\, \text{ind}\, (x-1) \equiv 4 \pmod{12},$$

于是

$$\text{ind}\,(x-1)\equiv 2,\ 8\,(\text{mod}\ 12),$$

查表得

$$x-1\equiv 4,\ 9\,(\text{mod}\ 13),$$

因此所求解为

$$x\equiv 5,\ 10\,(\text{mod}\ 13).$$

作为指标的一个应用，我们来讨论一般二项同余方程

$$x^n\equiv a\,(\text{mod}\ m),\qquad (1)$$

下面定理与§5.1中的类似，是讨论(1)有解条件及解的个数.

定理 1 假定 $(a,\ m)=1$，那末（1）有解的必要充分条件是

$$a^{\frac{\varphi(m)}{d}}\equiv 1\,(\text{mod}\,m)，\text{或ind}a\equiv 0\,(\text{mod}d)$$

这里 $d=(n,\ \varphi(m))$. 假如(1)有解，那末它就有 d 个关于模 m 不相同的解.

证明 因为(1)与

$$n\,\text{ind}\,x\equiv\text{ind}\,a\ (\text{mod}\ \varphi(m))\qquad (2)$$

等价，显然(2)有解的必要充分条件是

$$d=(n,\ \varphi(m))\ |\ \text{ind}\,a,$$

即
$$\text{ind}a\equiv 0\,(\text{mod}d)$$

于是
$$\frac{\varphi(m)}{d}\text{ind}\,a\equiv 0\ (\text{mod}\ \varphi(m))$$

或
$$\text{ind}\,a^{\frac{\varphi(m)}{d}}\equiv 0\,(\text{mod}\,\varphi(m))$$

所以
$$a^{\frac{\varphi(m)}{d}}\equiv 1\ (\text{mod}\,m)$$

假如同余方程(2)有解，那它就有 d 个关于模 $\varphi(m)$ 不

相同的 $\operatorname{ind} x$，因此，就有 d 个关于模 m 不相同的 x，这就是说假如（1）有解，它就有 d 个解，因此定理成立.

同第 5 章一样，当（1）有解时，a 叫做 m 的 n 方剩余，当（1）无解时，a 叫做 m 的 n 方非剩余.

定理 2 假如 m 的原根存在，那末在 m 的简化剩余系中，m 的 n 方剩余有 $\frac{\varphi(m)}{d}$ 个，这里 $d=(n, \varphi(m))$.

证明 假设 g 是 m 的原根，如果 g^t 是同余方程

$$x^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m,$$

的解，那末

$$g^{\frac{t}{d}\varphi(m)} \equiv 1 \pmod m$$

因此 $d \mid t$，因为自 1 到 $\varphi(m)$ 中 d 的倍数恰有 $\frac{\varphi(m)}{d}$ 个，所以这样的 g^t 恰有 $\frac{\varphi(m)}{d}$ 个，由上定理这 $\frac{\varphi(m)}{d}$ 个 g^t 都是 n 方剩余，因此定理成立.

§5.1 的定理 2，定理 1 是上定理 1，定理 2 的特例，因此我们说它们是 §5.1 的推广.

于是假如 p 是质数，$d=(n, p-1)$，那末在 p 的简化剩余系中有 $\frac{p-1}{d}$ 个 n 方剩余.

我们知道假如 $(a, m)=1$，如果 $x^n \equiv a \pmod m$ 有解，显然 $x^d \equiv a \pmod m$，$d=(n, \varphi(m))$，也有解. 反过来，如果 $x^d \equiv a \pmod m$ 有解，因为 $d=rn+s\varphi(m)$，所以 $x^d=x^{rn} \cdot x^{s\varphi(m)} \equiv x^{rn} \pmod m$，即 $(x^r)^n \equiv a \pmod m$，所以 $x^n \equiv a \pmod m$ 有解. 这就是说，假如 a 是 m 的 n 方剩余，那末 a 也是 m 的 d 方剩余. 反过来也成立. 因此，只要 n 不能整除 $\varphi(m)$，那末 m 的 n 方剩余就可以化为 m 的 $d(<n)$ 方剩余. 于是讨论 m 的 n

方剩余时主要是讨论$n\mid\varphi(m)$时的情况. 譬如质数$p=3k+1$时，那末p的3方剩余就是p的剩余. 因为这时$d=(3,3k)=3$,所以任意数都是p的3方剩余,再如果质数$p=4k+3$,那末p的4方剩余就是p的平方剩余，因为$d=(4,4k+2)=2$.

例 3 解 $x^8\equiv23\pmod{41}$.

解 这时$(8,40)=8$，由计算

$$23^{\frac{40}{8}}\equiv23^5\not\equiv1\pmod{41},$$

所以同余方程无解，也就是说23是41的8方非剩余.

例 4 解 $x^{12}\equiv37\pmod{41}$.

解 这时$(12,40)=4$，因为11是41的一个原根,由计算我们有

$11^2\equiv-2$，$11^4\equiv4$，$11^8\equiv16$，$11^{10}\equiv-32\equiv9$,

$11^{20}\equiv81\equiv-1$，$11^{24}\equiv-4\equiv37$,

所以 $\mathrm{ind}\,37=24$，即 $\mathrm{ind}\,37\equiv0\pmod4$，因此同余方程有解，即37是41的12方剩余. 下面来解方程.

取指标得

$$12\,\mathrm{ind}\,x\equiv\mathrm{ind}\,37=24\pmod{40},$$

即

$$3\,\mathrm{ind}\,x\equiv6\pmod{10},$$

因此

$$\mathrm{ind}\,x\equiv2\pmod{10},$$

所以关于模40，我们有

$$\mathrm{ind}\,x\equiv2,\ 12,\ 22,\ 32.$$

于是所求的4个解为

$$x \equiv 11^2,\ 11^{12},\ 11^{22},\ 11^{32},$$

即

$$x \equiv 39,\ 23,\ 2,\ 18\ (\bmod 41)。$$

解毕。

有时求解 (1) 化为求解 $x^d = b(\bmod m)$ 较为简便，这里 $d=(n,\ \varphi(m))$. 这是因为由 $d=rm+s\varphi(m)$，得 $x^{rn} \equiv x^d$，即 $x^d \equiv a^r \equiv b(\bmod m)$. 特别当 $d=1$ 时，x 可立即求出.

例 5 解 $x^{35} \equiv 17\quad (\bmod 67)$

解 因为 $\quad d=(35,\ 66)=1=35\cdot 17+66(-9)$,

所以 $\quad x \equiv x^{35\cdot 17} \equiv 17^{17} \equiv 33\ (\bmod 67)$

例 6 假定 p 是奇质数，试证 $\operatorname{ind}(-1)=\frac{p-1}{2}$.

证 假定 g 是 p 的原根，那末

$$g^{p-1}-1=(g^{\frac{p-1}{2}}-1)(g^{\frac{p-1}{2}}+1) \equiv 0(\bmod\ p),$$

因为 g 是 p 的原根，所以 $g^{\frac{p-1}{2}}-1 \not\equiv 0\ (\bmod p)$，因此

$$g^{\frac{p-1}{2}}+1 \equiv 0\ (\bmod p)$$

即

$$\operatorname{ind}(-1)=\frac{p-1}{2}.$$

习 题 6.4

1. 在 19 的简化剩余系中指出它的平方剩余及立方剩余.

2. 解下列各同余方程

1) $x^{35}\equiv 17 \pmod{67}$；

2) $x^{3}\equiv 23 \pmod{109}$；

3) $3^{x}\equiv 5 \pmod{13}$.

3. 假定 p 是奇质数，$a+b=p$，试证

$$\operatorname{ind} a-\operatorname{ind} b\equiv \frac{p-1}{2} \pmod{(p-1)}.$$

4. 假定 g，h 是质数 p 的两个不相同的原根，试证

$$\operatorname{ind}_h a\equiv \operatorname{ind}_g a\cdot \operatorname{ind}_h g \pmod{(p-1)}.$$

附　　录

4000 以下的质数与其最小原根表

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	101	2	233	3	383	5	547	2	701	2	877	2
3	2	03	5	39	7	89	2	57	2	09	2	81	3
5	2	07	2	41	7	97	5	63	2	19	11	83	3
7	3	09	6	51	6	401	3	69	3	27	5	87	5
11	2	13	3	57	3	09	21	71	3	33	6	907	2
13	2	27	3	63	5	19	2	77	5	39	3	11	17
17	3	31	2	69	2	21	2	87	2	43	5	19	7
19	2	37	3	71	6	31	7	93	3	51	3	29	3
23	5	39	2	77	5	33	5	99	7	57	2	37	5
29	2	49	2	81	3	39	15	601	7	61	6	41	2
31	3	51	6	83	3	43	2	07	3	69	11	47	2
37	2	57	5	93	2	49	3	13	2	73	2	53	3
41	6	63	2	307	5	57	13	17	3	87	2	67	5
43	3	67	5	11	17	61	2	19	2	97	2	71	6
47	5	73	2	13	10	63	3	31	3	809	3	77	3
53	2	79	2	17	2	67	2	41	3	11	3	83	5
59	2	81	2	31	3	79	13	43	11	21	2	91	6
61	2	91	19	37	10	87	3	47	5	23	3	97	7
67	2	93	5	47	2	91	2	53	2	27	2	1009	11
71	7	97	2	49	2	99	7	59	2	29	2	13	3
73	5	99	3	53	3	503	5	61	2	39	11	19	2
79	3	211	2	59	7	09	2	73	5	53	2	21	10
83	2	23	3	67	6	21	3	67	2	57	3	31	14
89	3	27	2	73	2	23	2	83	5	59	2	33	5
97	5	29	6	79	2	41	2	91	3	63	5	39	3

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1049	3	1229	2	1429	6	1597	11	1783	10	1993	5	2161	23
51	7	31	3	33	3	1601	3	87	2	97	2	79	7
61	2	37	2	39	7	07	5	89	6	99	3	2203	5
63	3	49	7	47	3	09	7	1801	11	2003	5	07	5
69	6	59	2	51	2	13	3	11	6	11	3	13	2
87	3	77	2	53	2	19	2	23	5	17	5	21	2
91	2	79	3	59	5	21	2	31	3	27	2	37	2
93	5	83	2	71	6	27	3	47	5	29	2	39	3
97	3	89	6	81	3	37	2	61	2	39	7	43	2
1108	5	91	2	83	2	57	11	67	2	53	2	51	7
09	2	97	10	87	5	63	3	71	14	63	5	67	2
17	2	1301	2	89	14	67	2	73	10	69	2	69	2
23	2	03	6	93	2	69	2	77	2	81	3	73	3
29	11	07	2	99	2	93	2	79	6	83	2	81	7
51	17	19	13	1511	11	97	3	89	3	87	5	87	19
53	5	21	13	23	2	99	3	1901	2	89	7	93	2
63	5	27	3	31	2	1709	3	07	2	99	2	97	5
71	2	61	3	43	5	21	3	13	3	2111	7	2309	2
81	7	67	5	49	2	23	3	31	2	13	5	11	3
87	2	73	2	53	3	33	2	33	5	29	3	33	2
93	3	81	2	59	19	41	2	49	2	31	2	39	2
1201	11	99	13	67	3	47	2	51	3	37	10	41	7
13	2	1409	3	71	2	53	7	73	2	41	2	47	3
17	3	23	3	79	3	59	6	79	2	43	3	51	13
23	5	27	2	83	5	77	5	87	2	53	3	57	2

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2371	2	2617	5	2803	2	3061	6	3319	6	3541	7	3769	7
77	5	21	2	19	2	67	2	23	2	47	2	79	2
81	3	33	3	33	5	79	6	29	3	57	2	93	5
83	5	47	3	37	2	83	2	31	3	59	3	97	2
89	2	57	3	43	2	89	3	43	5	71	2	3803	2
93	3	59	2	51	2	3109	6	47	2	81	2	21	3
99	11	63	5	57	11	19	7	59	11	83	3	23	3
2411	6	71	7	61	2	21	7	61	22	93	3	33	3
17	3	77	2	79	7	37	3	71	2	3607	5	47	5
23	5	83	2	87	5	63	3	73	5	13	2	51	2
37	2	87	5	97	3	67	5	89	3	17	3	53	2
41	6	89	19	2903	5	69	7	91	3	23	5	63	5
47	5	93	2	09	2	81	7	3407	5	31	21	77	2
59	2	99	2	17	5	87	2	13	2	37	2	81	13
67	2	2707	2	27	5	91	11	33	5	43	2	89	11
73	5	11	7	39	2	3203	2	49	3	59	2	3907	2
77	2	13	5	53	13	09	3	57	7	71	13	11	13
2503	3	19	3	57	2	17	5	61	2	73	5	17	2
21	17	29	3	63	2	21	10	63	3	77	2	19	3
31	2	31	3	69	3	29	6	67	2	91	2	23	2
39	2	41	2	71	10	51	6	69	2	97	5	29	3
43	5	49	6	99	17	53	2	91	2	3701	2	31	2
49	2	53	3	3001	14	57	3	99	2	09	2	43	3
51	6	67	3	11	2	59	3	3511	7	19	7	47	2
57	2	77	3	19	2	71	3	17	2	27	3	67	6
79	2	89	2	23	5	99	2	27	5	33	2	89	2
91	7	91	6	37	2	3301	6	29	17	39	7		
93	7	97	2	41	3	07	2	33	2	61	3		
2609	3	2801	3	49	11	13	10	39	2	67	5		

习 题 解 答

习 题 1.1

1. $la \pm ka = (l \pm k)a$.

2. $|ka| = |k||a| \geqslant |a|$, 因为 $|k| \geqslant 1$.

3. 因为 $a = 10q + b$, 而 $5 | b$, 所以 $5 | a$.

4. 因为 $(2n+1)^2 - 1 = 2n \cdot 2(n+1) = 4n(n+1)$.

5. $n = 3q + r$, $r = 0, 1, 2$. 当 $r = 0$ 时, $3 | n$; 当 $r = 1$ 时, $2n = 6q + 2$, 因此 $3 | (2n+1)$; 当 $r = 2$ 时, $3 | (n+1)$.

6. 用反证法, 假定 $d \geqslant b$, 即推得 $a > b^2$, 这与假设矛盾.

8. $1112 = (788)_{12}$, $1112 = (10001011000)_2$

9. 因 $d_1 = 1$, d_2, $\cdots$, $d_k = n$ 是 n 的所有正约数, 所以 $\frac{n}{d_1}$, $\frac{n}{d_2}$, $\cdots$, $\frac{n}{d_k}$ 也是 n 的所有正约数, 因此 $d_1 d_2 \cdots d_k = \frac{n}{d_1} \cdot \frac{n}{d_2} \cdots \frac{n}{d_k}$, 即 $(d_1 d_2 \cdots d_k)^2 = n^k$.

习 题 1.2

1. $(24871, 3468) = 17$, $(120, 504, 882) = 6$, $[135, 513, 3114] = 887490$.

2. 因为 $n^3 - n = (n-1)n(n+1)$ 是三个相邻数的乘积, 所以它是 3 的倍数, 再因为 n 是奇数, 所以 $n-1$, $n+1$ 都是偶数并且其中有一是 4 的倍数. 因此 $(n-1)(n+1)$ 是 8 的倍数, 所以 $n^3 - n$ 是 $3 \times 8 = 24$ 的倍数.

3. $(a, b)|a$, $(a, b)|b$, 所以 $(a, b)|c$.

4. 设 b 是公约数, d 是最大公约数, $[b, d]=c$, 那末 $d\leqslant c$, 又因为 $b|a_i$, $d|a_i$, 所以 $c|a_i$ 因此 c 是 $a_1, \cdots, a_n, \cdots$ 的公约数, 但 d 是最大公约数, 所以 $c\leqslant d$, 于是 $c=d$, 所以 $b|d$.

5. $(a_1, a_2)=1$ 时 $[a_1, a_2]=a_1a_2$. 同样 $[a_1, a_2, a_3]=[[a_1, a_2], a_3]=[a_1a_2, a_3]=a_1a_2a_3$.

6. 由 $\left(\frac{m}{a}, \frac{m}{b}\right)=1$ 得 $\left(\frac{m}{a}\cdot\frac{m}{b}, \frac{m}{a}+\frac{m}{b}\right)=1$, 即

$m(m, a+b)=ab$, 所以 $(m, a+b)=\frac{ab}{m}=(a, b)$.

7. 因为在数列 $a, 2a, \cdots, ba$ 中任意数都是 a 的倍数, 所以凡是 b 的倍数又都是 a, b 的最小公倍 $[a, b]$ 的倍数, 因此数列中 b 的倍数的个数 $=\frac{ba}{[a, b]}=(a, b)$.

8. 设 $x=8a$, $y=8b$, $(a, b)=1$, 因为 $(x, y)[x, y]=xy$, 所以 $8\cdot 64=64ab$, 即 $ab=8$, 于是 $a=1$ 或 $a=8$, 因此 $x=8$, $y=64$ 或 $x=64$, $y=8$.

9. $(a, b)^2=(a, b)(a, b)=(a(a, b), b(a, b))=(a^2, ab, b^2)=(a^2, b^2)$. 同样 $[a, b]^2=[a, b][a, b]=[a^2, ab, b^2]=[a^2, b^2]$.

10. $(a, b)(a, c)=(a^2, ac, ba, bc)=(a^2, a(b, c), bc)=(a^2, a, bc)=(a, bc)$.

11. 两边引用定理 2.

12. 设 $(a-b, a+b)=d$, 则 $a-b=kd$, $a+b=ld$. 于是 $2a=(k+l)d$, $2b=(k-l)d$. 因此 $2=(2a, 2b)=d(k+l, k-l)$, 即 $d|2$.

13. 因为 $1=(a_1+a_2,\ a_1b_2-a_2b_1)=(a_1+a_2,\ a_1b_2+a_1b_1)$ $=(a_1+a_2,\ b_1+b_2)$.

14. 设 $d_o=ax_o+by_o$ 是形如 $f(x,\ y)$ 的最小正数，显然 $d\,|\,d_o$，因此 $d\leqslant d_o$，又由§1.2定理6，$d=ax+by$，因为 d_o 是最小，所以 $d\geqslant d_o$，因此 $d=d_o$.

习 题 1.3

1. $T(2160)=40$，$S(2160)=7440$.

2. $p\,|\,r!\ c_p^r$，$r<p$，所以 $p\,|\,c_p^r$.

3. 假设 $(x,\ y)=d$，即 $x=dx_1$，$y=dy_1$，$(x_1,\ y_1)=1$ 那末 $x_1^2+y_1^2=ax_1y_1$，因此 $x_1\,|\,y_1^2$，$y_1\,|\,x_1^2$，所以 $x_1=y_1=1$ 于是 $a=2$.

4. 1) $3\,|\,a^2$，$3\,|\,b^2$ 则 $3\,|\,a$，$3\,|\,b$. 2) $3\nmid a^2$，$3\nmid b^2$，设 $a=3k+r, b=3l+s$，则 $a^2+b^2=9k^2+6kr+9l^2+6ls+r^2+s^2$，所以 $3\,|\,(r^2+s^2)$，但 $r=1$，2，时，$r^2=1$，4，于是 $r^2+s^2=2$，5，8，它不是3的倍数，此不可.

5. $T(a)=\prod\limits_{i=1}^{K}(a_i+1)=10$. 所以 $(a_1+1)(a_2+1)=1\cdot 10$ 或 $(a_1+1)(a_2+1)=2\cdot 5$，前者 $a_1=0$，$a_2=9$ 因此 $a=p_1^9$；后者 $a_1=1$，$a_2=4$，因此 $a=p_1p_2^4$，于是所求最小正数 $a=3\cdot 2^4=48$.

6. $S(a)=\dfrac{p_1^{a_1+1}-1}{p_1-1}\cdot\dfrac{p_2^{a_2+1}-1}{p_2-1}=15$，所以 $p_1=2$，$a_1=3$，即 $a=2^3=8$.

7. $a^{\frac{1}{2}T(a)}=64=2^6$，即 $a^{T(a)}=2^{12}$. 命 $a=2^{a_1}$，因为 $T(a)=a_1+1$，所以 $2^{a_1(a_1+1)}=2^{12}$，$a_1(a_1+1)=12$，即 $a_1=3$

或 $a_1=-4$ 所以 $a=2^3=8$.

8. $a^{\frac{1}{2}T(a)-1}=a$，即 $a^{\frac{1}{2}T(a)}=a^2$，所以 $T(a)=4$，于是

$(a_1+1)(a_3+1)=4$，因此 $a_1=3$，$a_2=0$ 或 $a_1=1$，$a_2=1$，即 $a=p^3$ 或 $a=pq$.

9. 假定 $b\geqslant c$，当 $a\geqslant b\geqslant c$ 时，$\max(\min(a, b), \min(a, c))=\max(b, c)=b$，$\min(a, \max(b, c))=\min(a, b)=b$. 因此所给等式成立. 当 $b\geqslant a\geqslant c$ 及 $b\geqslant c\geqslant a$ 时，同样证明.

10. 根据上题证明

11. 譬如，a 象下面这样取就可以

$$a=2\cdot3\cdots(k+1)t+2, \quad t=1, 2, \cdots.$$

12. 设不大于 n 的质数为 $p_1\cdots$，p_K，作 $q=p_1\cdots p_K-1$，显然 q 有异于 p_i 的质因数 p，所以 $p>n$. 又 $p<q<n!-1<n!$

13. 假定 p_1，p_2，$\cdots$，p_r 是形如 $3n+2$ 的质数，设 $a=3p_1p_2\cdots p_r-1=q_1q_2\cdots q_s$，这里 q_i 是质数，显然 q_i 与 3，p_1，p_2，$\cdots$，p_r 不相等，如果所有的 q_i 都是 $3n+1$ 的形状，那末它们的乘积 a 也是 $3n+1$ 的形状这与 $a=3p_1p_2\cdots p_r-1$ 矛盾. 所以至少有一 q_i 是 $3n+2$ 的形状.

14. 1) 9 个，

2) 90 个，

3) $n=2k$ 时有 $9\cdot10^{k-1}$ 个，$n=2k-1$ 时有 $9\cdot10^{k-1}$ 个.

习 题 1.4

1. 不超过 F_n 的费马数有 F_0，F_1，$\cdots$，F_n 共 $n+1$ 个，

每个有一质因数，由定理 5，它们不相等.

2. $(M_p, M_2)=1$，$M_2=3$. $(M_p, M_3)=1$，$M_3=7$.

习 题 1.5

1. $5(1000!)=200+40+8+1=249$，$\frac{1000}{2}=500$，所以 1000! 中有 249 个 0.

2. 不大于 30 的质数有：2, 3, 5, 7, 11, 13, 17, 19, 23, 29 等 10 个，$2(30!)=26$，$3(30!)=14$，$5(30!)=7$，$7(30!)=4$，$11(30!)=2$，$13(30!)=2$，$17(30!)=1$，$19(30!)=1$，$23(30!)=1$，$29(30!)=1$，所以

$$30!=2^{26}\cdot3^{14}\cdot5^{7}\cdot7^{4}\cdot11^{2}\cdot13^{2}\cdot17\cdot19\cdot23\cdot29.$$

3. $\left[\frac{545}{13}\right]=41$，$\left[\frac{176}{13}\right]=13$，所求数 $=41-13=28$.

4. $m=2^r-1$，$\left[\frac{m}{2}\right]=2^{r-1}-1$，$\left[\frac{m}{2^2}\right]=2^{r-2}-1$，…，$\left[\frac{m}{2^{r-1}}\right]=2-1=1$. 所以

$$2((2^r-1)!)=2^{r-1}+2^{r-2}+\cdots+2+1-r$$

$$=\frac{2^r-1}{2-1}-r=2^r-r-1.$$

5. $\left[\frac{n}{3}\right]+\left[\frac{n}{3^2}\right]+\cdots=7$，当 $n=18$ 时，$3(n!)=8$；当 $n=17$ 时，$3(n!)=6$，因此这样的 n 不存在.

6. 因为 $[x]\leqslant x<[x]+1$，所以 $[x]+a\leqslant x+a<[x]+a+1$，因此 $[x+a]=[x]+a$.

7. $a=[a]+r$，$b=[b]+s$，则 $a-b=[a]-[b]+r-s$，$r-s<1$. 当 $r-s\geqslant0$ 时，$[a-b]=[a]-[b]$；当 $r-s<0$ 时，

$[a-b]=[a]-[b]-1.$

8. 设 $n=n_1+n_2+\cdots+n_k$，因为

$$\frac{n}{p^i}=\frac{n_1}{p^i}+\frac{n_2}{p^i}+\cdots+\frac{n_k}{p^i},$$

所以 $$\left[\frac{n}{p^i}\right]\geqslant\left[\frac{n_1}{p^i}\right]+\left[\frac{n_2}{p^i}\right]+\cdots+\left[\frac{n_k}{p^i}\right].$$

于是 $$\Sigma\left[\frac{n}{p^i}\right]\geqslant\Sigma\left[\frac{n_1}{p^i}\right]+\Sigma\left[\frac{n_2}{p^i}\right]+\cdots+\Sigma\left[\frac{n_k}{p^i}\right],$$

即 p 在 $n!$ 中的最高幂不小于 p 在 $n_1!n_2!\cdots n_k!$ 中的最高幂，所以它是整数.

9. 对于正整数 $r(1\leqslant r\leqslant b-1)$，设 $\frac{r}{b}a=n+\frac{a'}{b}$ $(0<a'<b)$，那末 $\frac{a'}{b}<1$. 于是

$$\left[-\frac{r}{b}a\right]=-(n+1)=-\left[\frac{r}{b}a\right]-1$$

$$\left[\frac{b-r}{b}a\right]=\left[a-\frac{r}{b}a\right]=a+\left[-\frac{r}{b}a\right]$$

$$=a-\left[\frac{r}{b}a\right]-1=a-1-\left[\frac{r}{b}a\right]$$

因此 $$\sum_{r=1}^{b-1}\left[\frac{r}{b}a\right]=\sum_{r=1}^{b-1}\left[\frac{b-r}{b}a\right]=(b-1)(a-1)-\sum_{r=1}^{b-1}\left[\frac{r}{b}a\right].$$

所以 $$\sum_{r=1}^{b-1}\left[\frac{r}{b}a\right]=\frac{(b-1)(a-1)}{2}.$$

10. 因为 $\left[(3m+1)\cdot\frac{4}{3}\right]=\left[4m+1+\frac{1}{3}\right]=4m+1.$

习　题　2.1

1. $a=mk+b$，则 $(a,m)=(mk+b,m)=(b,m)$.

2. $10\equiv -1(11)$，$10^2\equiv 1(11)$，$10^3\equiv -1(11)$，…，

所以　$n=a_0+a_1 10^1+a_2 10^2+\cdots\equiv a_0-a_1+a_2-\cdots(11)$

即　$$(a_0+a_2+\cdots)-(a_1+a_3+\cdots)\equiv 0(11).$$

4. $1000\equiv -1(13)$，同例 3 完全一样，得

$$(a_0+a_2+\cdots)\equiv(a_1+a_3+\cdots)(13).$$

今 $637693=693-637\cdot 1000$，$a_0-a_1=693-637=56\not\equiv 0(13)$，所以它不能被 13 整除.

5. $a\equiv 8(9)$，$b\equiv 3(9)$，$c\equiv 5(9)$，但 $ab\equiv 24\not\equiv 5(9)$，所以结果是错误的.

6. 用二项式定理，得

$$(a+b)^p=a^p+\frac{p}{1}a^{p-1}b+\frac{p(p-1)}{2}a^{p-2}b^2+\cdots+\frac{p}{1}ab^{p-1}+b^p,$$

因此 $(a+b)^p-(a^p+b^p)=p\left(a^{p-1}b+\frac{p-1}{2}a^{p-2}b^2+\cdots+ab^{p-1}\right)$,

所以　$$(a+b)^p-(a^p+b^p)\equiv 0(\bmod p).$$

习　题　2.2

1. $a^{p-1}\equiv 1(p)$，$p-1\equiv -1(p)$，$(p-1)^a\equiv(-1)^a(p)$，因此当 a 是奇数时　$a^{p-1}+(p-1)^a\equiv 0(p)$；当 a 是偶数时，$a^{p-1}-(p-1)^a\equiv 0(p)$.

2. $2n(2n+2)=4n(n+1)$，$2|n(n+1)$，所以 $8|2n(2n+2)$. $p^4-1=(p-1)(p+1)(p^2+1)$，$240=2^4\cdot 3\cdot 5$. 因 $8|(p-1)\cdot(p+1)$，$p^2\equiv 1(3)$，即 $3|(p-1)(p+1)$，又因为 $2|(p^2+1)\cdot$

$p^4\equiv1(5)$，即 $5|(p^4-1)$，所以 $240|(p^4-1)$.

3. $p^2-q^2=p^2-1-(q^2-1)$，因为 $3\ (p^2-1)$，$8|(p^2-1)$，所以 $24|(p^2-1)$. 同样 $24|(q^2-1)$，所以 $24|(p^2-q^2)$.

4. $p^6-1=(p^2-1)(\cdots)$，$168=2^3\cdot3\cdot7$，因 $p^6\equiv1(7)$，即 $7|(p^6-1)$，$3|(p^2-1)$，$8|(p^2-1)$，所以 $168|(p^6-1)$.

5. $x^{p-1}\equiv1(p)$，$x^{2(p-1)}\equiv1(p)$，又 $x^{2(p-1)}=x^{q-1}\equiv1(q)$，命 $p-1=2t$，则 $x^{2(p-1)}-1=(x^t)^4-1=(x^{2t}-1)(x^{2t}+1)$，于是 $8|(x^{2t}-1)$，$2|(x^{2t}+1)$，所以 $x^{2(p-1)}\equiv1(16pq)$

6. $p^{q-1}\equiv1(q)$，所以 $p^{q-1}+q^{p-1}\equiv1(q)$，同样 $q^{p-1}+p^{q-1}\equiv1(p)$ 所以 $p^{q-1}+q^{p-1}\equiv1(pq)$.

习 题 2.3

1. $\varphi(60)=16$，$1956=122\cdot16+4$，所以 $13^{1956}\equiv13^4=(169)^2=(-11)^2=121\equiv1(60)$.

2. 设 $m=p_1^{m_1}\cdots p_r^{m_r}$，则 $\varphi(m)=p_1^{m_1-1}\cdots p_r^{m_r-1}(p_1-1)\cdots(p_r-1)$，当 $\varphi(m)$ 是奇数时 p_i 不能为奇数，因此 $p_1=2$，$m_1=1$，即 $m=2$. 显然还有 $m=1$.

3. 证法与上题类似.

4. 设 $x=p_1^{a_1}\cdots p_r^{a_r}$，则

$$\varphi(x)=p_1^{a_1-1}\cdots p_r^{a_r-1}(p_1-1)\cdots(p_r-1)=2(2n-1),$$

显然 $r=1$，即 $p_1^{a_1-1}(p_1-1)=2(2n-1)$. 因为 $p_1-1\not\equiv0(4)$，$p_1-1\not\equiv1(4)$，$p_1-1\not\equiv3(4)$，所以 $p_1-1\equiv2(4)$. 于是 $p_1=4k-1$，因此 $x=p_1^{a_1}$ 或 $x=2p_1^{a_1}$.

5. 根据完全剩余系定义证明.

6. 当 $\frac{m}{n}$ 是既约真分数时，m 是 n 的简化剩余系中数.

7. $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, …, $\frac{m_i}{n}$, …, $\frac{m_{\varphi(n)}}{n}$共计 $\varphi(2)+\varphi(3)+\cdots+\varphi(n)$个.

8. 引用定理 4.

9. 引用定理 2，容易证得 $d\varphi(a)\varphi(b)=\varphi(ab)\cdot\varphi(d)$.

10. 假如 m_1, …, $m_{\varphi(m)}$ 是 m 的简化剩余系，那末 $m-m_1$, …, $m-m_{\varphi(m)}$ 也是 m 的简化剩余系，于是 $(m-m_1)+\cdots+(m-m_{\varphi(m)})=m_1+\cdots+m_{\varphi(m)}$，即 $m\varphi(m)=2(m_1+\cdots+m_{\varphi(m)})$，所以 $m_1+\cdots+m_{\varphi(m)}=\frac{m\varphi(m)}{2}$.

11. 设 p_1, …, p_k 是 m 的互异质约数，因为 $\phi(m)=m\prod\limits_{i=1}^{k}\frac{p_i-1}{p_i}$ 所以 $\Pi\frac{p_i-1}{p_i}=\frac{1}{p}$ 即 $p\Pi(p_i-1)=p_1\cdots p_k$，假定 p_1 是 p_1, …, p_k 中最大数，那末 $p_1|p$，因此 $p_1=p$. 于是 $\Pi(p_i-1)=p_2\cdots p_k$，因为 p_i-1 是偶数，所以 p_1, …, p_k 中奇数不能多于 1 个. 于是当 p_1, …, p_k 没有奇数时 $p_1=2$，当 p_1, …, p_k 中有一是奇数时，其中还一定有一个偶数，这时 $p_1=3$，$p_2=2$. 于是所求数为

$p=2$，$m=2^k$ 或 $p=3$，$m=2^k3^l$，k，l 是任意正整数.

12. 设 $\varphi(y)=r$，当 $x>2$ 时，$r=\varphi(x^{\phi(y)})>x^{\phi(y)-1}=x^{r-1}$ 即 $r>x^{r-1}$，$x>2$，这显然是矛盾. 所以 $x\leqslant 2$，于是所求解为

$$\begin{cases}x=1\\y=1\end{cases}\quad\begin{cases}x=2\\y=2\end{cases}\quad\begin{cases}x=2\\y=4\end{cases}$$

习 题 3.1

1. 1) $\begin{cases} x = 8 + 11t, \\ y = -18 - 25t \end{cases}$

2) $\begin{cases} x = 4 - 9t_1 - 10t_2 \\ y = 2 - 4t_1 - 5t_2 \\ z = 2 \qquad - t_2 \end{cases}$

3) $\begin{cases} x = -18 - 54c + 21b + 5a \\ y = 6 + 18c - 7b - 2a \\ z = 1 + 3c - b \\ t = 3 - c \end{cases}$

2. 1) 有五组解，其中 $x = 11$，31，51，71，91，

2) 由 $x(x+y) = 6$，得 $x = 1$，$y = 5$；$x = 2$，$y = 1$.

3) 把原式化成 $y = 2 + \frac{4}{x-1}$，所以 $x - 1 = 1, 2, 4$，即 $x = 2$，3，5.

3. 消去 x 得 $2y - z = 3$，解之得 $y = 2 + t$，$z = 1 + 2t$ 代入所给方程得 $x = 3 - 8t$.

4. 设 $4k+1$ 为两位数，因为 $10 \leqslant 4k + 1 < 100$，即 $2\frac{1}{4} \leqslant k < 24\frac{3}{4}$，所以 k 可取 3 与 24 之间的 22 个数，得 22 个成等差级数的二位数，其和为 1210.

5. $A = 7$，$B = 10$ 或 $A = 2$，$B = 23$.

6.

鸡翁	0	4	8	12
鸡母	25	18	11	4
鸡雏	75	78	81	84

7. 因为 $a^2xy+abx+acy+ad=0$ 可以写成 $(ax+c)(ay+b)=bc-ad$ 如果 $bc-ad\neq0$，那末 $ax+c$ 是 $bc-ad$ 的因式，因此 x 只能有有穷个整数解. 同样 y 也只能有有穷个解，所以只有 $bc-ad=0$ 时如果 $a|c$，那末 $x=-\frac{c}{a}$，y 取任意整数都是解，因此有无穷多组解，如果 $a|b$，同样也有无穷多组解.

习　题　3.2

1.

b	1	1	1	2	2	2	3	4
a	2	4	6	3	5	7	4	5
x	3	15	35	5	21	45	7	9
y	4	8	12	12	20	28	24	40
z	5	17	37	13	29	53	25	41

2. 设 $x-y=a^2$，$y-z=b^2$，$x-z=c^2$，则 $a^2+b^2=c^2$，因此给出 a，b 的值即求得 x，y，z.

3. 设 $p=x^2+y^2$，因为 x，$y\equiv0$，±1，$2(4)$，所以

$$x^2+y^2\equiv0,\ 1,\ 2(4)$$

但 $p\equiv3(4)$，因此 $p\neq x^2+y^2$.

4. 设 $x^2-60=y^2$，则 $(x-y)(x+y)=60$，因此 $x-y$ 及 $x+y$ 必同为偶数，于是 $x-y=2$，$x+y=30$ 或 $x-y=6$，

$x+y=10$，所以 $x=16$ 或 $x=8$.

5. 由 $x^2-5=y^2$，$x^2+5=z^2$ 得 $10=z^2-y^2=(z-y)(z+y)$. 但 $z-y$，$z+y$ 中有一为偶数，他一也为偶数，因此它们的积就是 4 的倍数，这不可. 所以这样的平方数 t 不存在.

6. 所给方程可写成 $(y-x)(x+y-1)=18$，由 $x\geqslant 1$，得 $2x-1>1$，于是 $x+y-1=(y-x)+2x-1>y-x$，因此 $y-x$ 可取 1，2，3 而 $x+y-1$ 应取 18，9，6，即

$$\begin{cases}y-x=1\\x+y-1=18\end{cases}\qquad\begin{cases}y-x=2\\x+y-1=9\end{cases}\qquad\begin{cases}y-x=3\\x+y-1=9\end{cases}$$

解之得

$$\begin{cases}x=9\\y=10\end{cases}\qquad\begin{cases}x=4\\y=6\end{cases}\qquad\begin{cases}x=2\\y=5\end{cases}$$

7. 因为 $z^4=(x^4-4y^4)^2=x^8-8x^4y^4+16y^8=(x^4+4y^4)^2-(2xy)^4$，即 $(2xy)^4+z^4=(x^4+4y^2)^2$.

8. 因为 $x^2+1=3y^2$，所以 x^2+1 是 3 的倍数，设 $x=3k$，$3k+1$，$3k+2$ 代入验证得知 x^2+1 都不是 3 的倍数，因此所给方程没有整数解.

9. 适当取正整数 x 使 $n-x^2=m$ 为一正奇数，设 $y=\frac{m+1}{2}$，因为 $y^2-m=\left(\frac{m-1}{2}\right)^2=z^2$，所以 $n-x^2=y^2-z^2$.

10. 设 a，b，c 是商高方程的任一组解，那末 $(ac^{n-1})^2+(bc^{n-1})^2=(c^2)^n$.

11. 因为 $\Sigma\{(2n^2+2n+i)^2-(2n^2+n+i)^2\}=\Sigma n(4n^2+3n+2i)=(2n^2+n)^2$ 所以给出的式成立. 取 $n=3$ 得 21^2+22^2

$+23^2+24^2=25^2+26^2+27^2$.

习 题 3.3

1. $365=13^2+14^2$, $1105=9^2+32^2$, $1961=19^2+40^2$
   $5461=43\cdot127$，不能写成平方数的和.

3. 因为 $m=a^2-b^2=(a-b)(a+b)$，

$$m=ab=\left(\frac{a+b}{2}\right)^2-\left(\frac{a-b}{2}\right)^2$$

4. 因为 $\left\{\frac{n(n+1)}{2}\right\}^2-\left\{\frac{(n-1)n}{2}\right\}^2=n^3$.

6. 设 $a=(2n)^2+(2n)^2$，$b=8n^2+1$，$c=(2n-1)^2+(2n+1)^2$，当 $n=\frac{m^2+m}{2}$时，$a=2m^2(m+1)^2$, $b=2m^2(m+1)^2+1$, $c=2m^2(m+1)^2+2$，即 a, b, c 是三个相邻数.

7. 设 $x=a+3d$，$y=a+4d$，$z=a+5d$，$\omega=a+bt$，代入所给方程得 $a(a^2+9ad+21d^2)=0$，因此 $a=0$，即所求数组为 $x=3d$，$y=4d$，$z=5d$，$\omega=6d$，这里 d 是任意正整数.

习 题 4.1

1. 1) $(256, 337)=1$，它有一个解 $x\equiv81(337)$
   2) $(1215, 2755)=5$，$5|560$，所以方程有 5 个解：
      $x\equiv200, 751, 1302, 1853, 2404(2755)$；
   3) $y=1+2t$，$x\equiv-1-5t+3s(\mathrm{mod}\ 18)$，$t=0, 1, \cdots, 8$；$s=0, 1, \cdots, 5$. 共 $9\times6=54$ 个解.

2. $x=4+49t$，$y=-3+37t$.

3. $x\equiv93(140)$.

4. 1) $x\equiv8(209)$；

2) $x\equiv -2(77)$.

5. $x\equiv 6$, $y\equiv -1$, $z\equiv -8(17)$.

6. $x=2531$.

7. 设 $\alpha\equiv a(m)$，即 $m|(\alpha-a)$，因此 $p_i^{m_i}|(\alpha-a)$， 所以 $\alpha\equiv a(p^{m_i})$. 反过来假如 $\alpha\equiv a(p_i^{m_i})$，即 $p_i^{m_i}|(\alpha-a)$， 因此 $\Pi p_i^{m_i}|(\alpha-a)$，所以 $\alpha\equiv a(m)$.

习　题　4.2

1. $x\equiv 0,\ 1,\ \pm 2(5)$.

2. $x\equiv 1,\ -2,\ \pm 3(7)$.

3. $x\equiv \pm 2,\ \pm 18(41)$.

4. 因为 $n|(p-1)$， 所以 $x^{p-1}-1=(x^n-1)g(x)$，这里 $g(x)$ 是次数为 $p-1-n$ 的 x 多项式，由定理1， $g(x)\equiv 0(\mathrm{mod}\ p)$至多只能有 $p-1-n$ 个解，但 $x^{p-1}\equiv 1(\mathrm{mod}\ p)$ 有 $p-1$ 个解，所以 $x^n-1\equiv 0(\mathrm{mod}\ p)$至少有 $p-1-(p-1-n)=n$ 个. 又由定理1不能比这多，所以恰好有 n 个解.

5. 假如 $f(x)\equiv 0(\mathrm{mod}\ p)$有 p 个不相同的解，由

$$f(x)=(x^p-x)q(x)+r(x),$$

显然 $r(x)\equiv 0(\mathrm{mod}\ p)$也有 p 个不相同解：但 $r(x)$ 的次数小于 p， 所以 $r(x)$ 的系数都是 p 的倍数， 于是 $f(x)\equiv(x^p-x)q(x)(\mathrm{mod}\ p)$即 x^p-x 是 $f(x)$关于模 p 的因式，反过来也成立.

习　题　4.3

1. $x\equiv 22(27)$.

2. 无解.

3. $x\equiv 1$, $7(25)$.

4. $x\equiv 2$, 5, 11, 17, 20, $26(30)$.

5. $x\equiv 1$, 4, 11, $14(15)$.

6. $x\equiv 93(125)$.

7. $x\equiv 91(120)$.

习 题 5.2

1. $\left(\frac{88}{109}\right)=1$, $\left(\frac{365}{1847}\right)=1$, $\left(\frac{-1457}{2389}\right)=-1$.

2. $\left(\frac{17}{23}\right)=-1$，所给不定方程无解.

3. 23 的平方剩余是

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 13,\ 16,\ 18$$

23 的平方非剩余是

$$5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22$$

4. 以 7 为平方剩余的奇质数

$$p=28n\pm 1,\ 28n\pm 3,\ 28n\pm 9,$$

以 7 为平方非剩余的奇质数

$$p=28n\pm 5,\ 28n\pm 11,\ 28n\pm 13.$$

5. 1) $\left(\frac{p}{q}\right)=\left(\frac{q+4a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{a}{q}\right)$;

2) $\left(\frac{q}{p}\right)=\left(\frac{p-4a}{p}\right)=\left(\frac{-4a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$.

因为 $p\equiv q \pmod 4$ 所以 $p\equiv 1 \pmod 4$ 或 $p\equiv -1 \pmod 4$. 当 $p\equiv 1 \pmod 4$ 时，$\left(\frac{-1}{p}\right)=+1$，$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$，当 $p\equiv -1$

$(\bmod 4)$时，$(\frac{-1}{p})=-1$，$(\frac{p}{q})=-(\frac{q}{p})$所以不论属何种情况总有$(\frac{a}{p})=(\frac{a}{q})$.

6. $(\frac{-1}{p})=1$ 时，$p\equiv 1(4)$，即 $p=4k+1$. 再 $p-1=4k$，$(p-1)!=(4k)!$ 于是 $1\cdot 2\cdots 2k(2k+1)(2k+2)\cdots 4k=1\cdot 2\cdots 2k(p-2k)(p-2k+1)\cdots(p-1)\equiv(1\cdot 2\cdots 2k)^2(\bmod p)$.

7. $x^2+3\equiv 0(p)$，$(\frac{-3}{p})=(\frac{-1}{p})(\frac{3}{p})=(\frac{p}{3})$，$p^{\frac{3-1}{2}}\equiv 1(3)$，因此 $p\equiv 1(3)$ 即 $p=1+3t$，因为 p 是奇数，所以 $t=2k$. 于是 $p=6k+1$.

8. $x^2\equiv -y^2(p)$，$(\frac{-y^2}{p})=(\frac{-1}{p})(\frac{y^2}{p})=(\frac{-1}{p})$，所以 $p=4n+1$.

$x^2\equiv 2y^2(p)$，$(\frac{2y^2}{p})=(\frac{2}{p})$，所以 $p=8n\pm 1$.

9. 假如 p_1，$\cdots$，p_n 是 n 个形状象 $4k+1$ 的质数，则 $(2p_1\cdots p_n)^2+1$ 的奇质因数也是 $4k+1$ 形状. 同样 $(2p_1\cdots p_n)^2+3$ 的奇质因数又是 $6k+1$ 形状.

习 题 5.4

1. $x\equiv\pm 9(19)$.
2. $x\equiv\pm 11(29)$.
3. $x\equiv\pm 12(71)$.
4. $x\equiv\pm 21(73)$.
5. $x\equiv\pm 94(353)$.
6. $x\equiv\pm 11(27)$.

习 题 5.5

1. $x\equiv\pm19$, $\pm19+32(64)$.

2. $x\equiv\pm108(343)$.

3. $x\equiv\pm41$, $\pm41+128(256)$.

4. $x\equiv\pm113$, $\pm141(508)$.

5. (3)的4个解 $x\equiv\pm a$, $\pm a+2^{k-1}(2^k)$ 当然都是(4)的解，这4个解关于模 2^k 是4个互不同余的解，但关于模 2^{k-1} 就只有二个互不同余的解，这就是说(3)的4个解只是(4)的二个解了．譬如 $x^2\equiv1(2^3)$ 的解是 ±1, $\pm1+4$，即1，3，5，9．而 $x^2\equiv1(2^4)$ 的解是 ±1, $\pm1+8$，即1，7，9，15．这时 $1\equiv9$, $7\equiv15(2^3)$.

习 题 6.1

1．1) $a^p\equiv1(q)$, $a^\lambda\equiv1(q)$，则 $\lambda|p$，因此 $\lambda=1$ 或 $\lambda=p$，当 $\lambda=1$ 时 $a-1\equiv0(q)$，即 $q|(a-1)$．当 $\lambda=p$ 时，$\lambda|\varphi(q)=q-1$，于是 $q=pt+1$ 但 q 是奇数，所以 $q=2pm+1$.

2) $a^p\equiv-1(q)$，即 $(-a)^p\equiv1(q)$．因此 $q|(-a-1)$，即 $q|(a+1)$ 或 $q=2pm+1$.

2．假定 g 是 p 的原根，那末1，g，g^2，…，g^{p-1} 是 p 的简化剩余系，但1，2，…，$p-1$ 也是 p 的简化剩余系．于是有 $1^n+2^n+\cdots+(p-1)^n\equiv1^n+g^n+g^{2n}+\cdots+g^{(p-2)n}$ $\equiv\dfrac{g^{(p-1)n}-1}{g^n-1}\pmod p$ 但 $g^{p-1}\equiv1\pmod p$，而 n 不是 $p-1$ 的约数，所以 $g^n-1\not\equiv0\pmod p$，于是所给式成立.

3．$a^\lambda\equiv1(m)$，$(a^k)^\mu\equiv1(m)$，则 $\lambda|k\mu$，命 $d=(\lambda,k)$

得 $\frac{\lambda}{d} \mid \mu$，再 $(a^k)^{\frac{\lambda}{d}} \equiv (a^\lambda)^{\frac{k}{d}} \equiv 1\ (m)$，于是 $\mu \mid \frac{\lambda}{d}$. 因此 $\mu = \frac{\lambda}{d}$.

4. 因为 $a^{\lambda_1} \equiv 1 \pmod{p_1}$，$a^{\lambda_2} \equiv 1 \pmod{p_2}$，于是 $(a^{\lambda_1})^{\frac{m}{\lambda_1}} \equiv 1 \pmod{p_1}$，$(a^{\lambda_2})^{\frac{m}{\lambda_2}} \equiv 1 \pmod{p_2}$，所以 $a^m \equiv 1 \pmod{p_1 p_2}$.

假如 a 关于模 $p_1 p_2$ 的阶数是 λ，那末 $\lambda \mid m$，再由于 $a^\lambda \equiv 1 \pmod{p_1 p_2}$，得

$$a^\lambda \equiv 1 \pmod{p_i},\ i = 1,\ 2.$$

因此 $\lambda_i \mid \lambda$，于是 $m \mid \lambda$. 所以 $\lambda = m$.

5. 设 a 是 p 的平方非剩余，那末 $a^{\frac{p-1}{2}} = a^{2^{m-1}} \not\equiv 1 \pmod{p}$，但 $a^{p-1} = a^{2^m} \equiv 1 \pmod{p}$，所以 a 的阶数是 $2^m = p-1$. 即 a 是 p 的原根.

习 题 6.2

1. 23 的原根共有 10 个：

$$5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21$$

54 的原根共有 6 个：5，11，23，29，41，47. 再 5 是 23 的原根，它也是 $529 = 23^2$ 的原根，又是 $1058 = 2 \cdot 23^2$ 的原根.

2. 设 g 的阶数是 λ，并且 $\lambda < p-1$ 则 $\lambda \mid (p-1)$. 命 $p-1 = \lambda d$. 如果 $2 \mid d$，即 $d = 2d_1$，于是 $\lambda d_1 = \frac{p-1}{2}$，$g^{\lambda d_1} = (g^\lambda)^{d_1} \equiv 1\ (p)$，即 $g^{\frac{p-1}{2}} \equiv 1\ (p)$，这与假设矛盾. 如果 $q_i \mid d$，即 $d = q_i d_i$，则 $\lambda d_i = \frac{p-1}{q_i}$，于是 $g^{\lambda d_i} \equiv (g^\lambda)^{d_i} \equiv 1\ (p)$，即 $g^{\frac{p-1}{q_i}} \equiv 1\ (p)$，这又与假设矛盾，因此 $\lambda = p-1$，所以 g 是 p 的原根.

3. 假定a是p的平方非剩余，a关于p的阶数是λ，则$\lambda|\varphi(p)=2^k$，如果$\lambda<2^k$，命$\lambda=2^l$，$l<k$，于是$a^{2^l}\equiv1(p)$，因此$a^{\frac{p-1}{2}}\equiv1(p)$，这与$a$是平方非剩余的假设不合，所以$\lambda=2^k=p-1$.

习　题　6.3

1. 2 由定理 2 立即推得.

习　题　6.4

1. 平方剩余为 1，4，5，6，7，9，11，16，17，立方剩余为 1，7，8，11，12，18.

2. 1) $x\equiv33(67)$；

   2) $x\equiv59, 11, 39(109)$；

   3) 无解.

3. $a\equiv-b(p)$，所以 $\mathrm{ind}\,a=\mathrm{ind}(-1)+\mathrm{ind}\,b$ 因此 $\mathrm{ind}\,a-\mathrm{ind}\,b\equiv\frac{p-1}{2}\ (p-1)$.

4. 设 $h^{l_1}\equiv a(p)$，$g^{l_2}\equiv a(p)$，$h^{l_3}\equiv g(p)$ 则 $h^{l_2l_3}\equiv g^{l_2}\equiv h^{l_1}(p)$ 所以 $l_1\equiv l_2l_3(p-1)$.